NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

USMC ACQUISITION STRATEGIES FOR COTS MOBILE DEVICES IN THE TACTICAL ENVIRONMENT

by

Samuel K. Hong
Nicholas S. Payne

September 2017

Thesis Advisor:	Douglas MacKinnon
Co-Advisor:	Raymond Jones
Second Reader:	John Gibson

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE USMC ACQUISITION STRATEGIES FOR COTS MOBILE DEVICES IN THE TACTICAL ENVIRONMENT			**5. FUNDING NUMBERS**
6. AUTHOR(S) Samuel K. Hong, Nicholas S. Payne			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) HQMC Aviation			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER** NPS-N16-M343-D
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The United States Marine Corps (USMC) has historically struggled to procure capabilities fast enough to take advantage of technological advances before they become obsolete. In particular, the USMC's operational requirements reflect an increasing demand to procure mobile devices that provide broadband secure capability at low cost and high volume. This research identified and assessed acquisition strategies to support rapid adoption and integration of emerging commercial off-the-shelf (COTS) mobile devices into the tactical domain. Procurement recommendations are provided from clearly identifying Department of Defense standards for mobile devices while analyzing current acquisition architectures through policy and regulation reviews. The scope of this research included traditional and non-traditional acquisition strategies and an examination of rapid acquisition organizations. This research concluded that, due to their requirements-based approach, current USMC acquisition strategies are being out-paced by the increasing speed of mobile device technology. Rapid procurement of mobile devices may be possible with a standards-based approach that sets minimum open standards for maximizing interoperability, competition, and cost savings. Due to the technology maturity, low development, and flexibility to tailor programs, the mobile device program may enter the acquisition process at Milestone C to go into operational testing and rapid fielding to the warfighter.

14. SUBJECT TERMS rapid, acquisition, COTS, mobile device, information technology			**15. NUMBER OF PAGES** 115
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

USMC ACQUISITION STRATEGIES FOR COTS MOBILE DEVICES IN THE TACTICAL ENVIRONMENT

Samuel K. Hong
Major, United States Marine Corps
B.S., University of California, Los Angeles, 2006

Nicholas S. Payne
Captain, United States Marine Corps
B.S., University of Maryland, College Park, 2011

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
September 2017

Approved by:

Dr. Douglas MacKinnon
Thesis Advisor

Raymond Jones
Co-Advisor

John Gibson
Second Reader

Dr. Dan Boger
Chair, Department of Information Sciences

Glenn Cook
Academic Associate
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The United States Marine Corps (USMC) has historically struggled to procure capabilities fast enough to take advantage of technological advances before they become obsolete. In particular, the USMC's operational requirements reflect an increasing demand to procure mobile devices that provide broadband secure capability at low cost and high volume. This research identified and assessed acquisition strategies to support rapid adoption and integration of emerging commercial off-the-shelf (COTS) mobile devices into the tactical domain. Procurement recommendations are provided from clearly identifying Department of Defense standards for mobile devices while analyzing current acquisition architectures through policy and regulation reviews. The scope of this research included traditional and non-traditional acquisition strategies and an examination of rapid acquisition organizations. This research concluded that, due to their requirements-based approach, current USMC acquisition strategies are being out-paced by the increasing speed of mobile device technology. Rapid procurement of mobile devices may be possible with a standards-based approach that sets minimum open standards for maximizing interoperability, competition, and cost savings. Due to the technology maturity, low development, and flexibility to tailor programs, the mobile device program may enter the acquisition process at Milestone C to go into operational testing and rapid fielding to the warfighter.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAS	assisted acquisition services
ACAT	acquisition category
ACTD	advanced concepts technology demonstration
AMF JTRS	airborne and maritime fixed station joint tactical radio system
AT&L	acquisition technology and logistics
ATO	authority to operate
ATTTB	alcohol and tobacco tax trade bureau
BYOD	bring your own device
C2	command and control
C&A	certification and accreditation
CAS	close air support
CDMA	code division multiple access
CIA	central intelligence agency
CIO	chief information officer
CMD	commercial mobile device
CMDWG	commercial mobile device working group
CND	computer network defense
CNSS	committee on national security systems
COTS	commercial off-the-shelf
CSfC	commercial solution for classified
CSO	commercial solutions opening
CUI	controlled unclassified information
DAMIR	defense acquisition management information retrieval
DARPA	Defense Advanced Research Projects Agency
DAS	Defense Acquisition System
DISA	Defense Information Systems Agency
DISN	defense information system network
DISR	DOD IT standards registry
DIUX	defense innovation unit experimental
DOD	department of defense

DODIN APL	Department of Defense information network approved products list
DOTMLPF	doctrine, organization, training and education, materiel, leadership, personnel, and facilities
EEOC	equal opportunity employment council
EMD	engineering & manufacturing development
EMS	emergency medical services
FAR	federal acquisition regulation
FDD	full deployment decision
FMR	financial management regulation
FRP	full-rate production
GAO	government accountability office
GIG	global information grid
GOTS	government-off-the-shelf
GPS	global positioning system
GSM	global system for mobile communication
HMS	handheld, manpack and small form fit
HQMC	Headquarters Marine Corps
IA	information assurance
IAM	identity and access management
IOC	initial operational capability
IOT&E	initial operational test and evaluation
IT	information technology
JCIDS	joint capabilities integration and development system
JCTD	joint capabilities technology demonstration
JIE	joint information environment
JITC	joint interoperability test command
JRAC	joint rapid acquisition cell
JTAC	joint terminal attack controller
KILSWITCH	kinetic integrated low-cost software integrated tactical common handheld
KPP	key performance parameters
LAN	local area network
LCSP	life cycle sustainment plan

LRIP	low-rate initial production
MAGTF	marine air ground task force
MAIS	major automated information systems
MAM	mobile application management
MARCORSYSCOM	Marine Corps systems command
MCCDC	Marine Corps combat development command
MCEN	marine corps enterprise network
MCWL	marine corps warfighting laboratory
MDD	material development decision
MDM	mobile device management
MOSA	modular open systems approach
OSD	office of the secretary of defense
NDAA	national defense authorization act
NATO	North Atlantic Treaty Organization
NFC	near field communication
NIAP	national information assurance partnership
NIST	national institute of standards and technology
NSA	national security administration
NSS	national security systems
O&S	operations and support
OEF	operation enduring freedom
OPSEC	operations security
OS	operating system
OT	other transactions
PC	personal computer
PCAS	persistent close air support
PCS	personal communication services
PDA	personnel digital assistant
PED	portable electronic device
PEO	program executive office
PEO C4I	program executive office for command, control, communications, computers, and intelligence
PIM	personal information manager

PIV	personal identity verification
PLI	position, location, identity
PM	program manager
PPBE	planning, programming, budgeting and execution
QIC	In-Q-Tel interface center
R&D	research and development
RD&D	research, development, and demonstration
RDD	risk reduction decision
REF	rapid equipping force
RPP	request for prototype proposal
RSTA	reconnaissance, surveillance and target acquisition
SBIR	small business innovation research
SCAP	security content automation protocol
SMS	short message service
SOW	statement of work
STTR	small business technology transfer
TEMP	test & evaluation master plan
TMRR	technology maturation & risk reduction
UNS	urgent needs statement
UON	urgent operational need
USMC	United States Marine Corps
USD	undersecretary of defense
VCSA	vice chief of staff of the Army
VPN	virtual private network

I. INTRODUCTION

A. BACKGROUND

Rapid emergence of mobile devices, including cell phones and tablets, has provided capabilities in small hand-held devices that were once only attainable in laptops and desktop computers. Due to their many benefits, demand for mobile devices in the United States Marine Corps (USMC) has increased significantly in recent years (United States Marine Corps [USMC], 2014). The USMC seeks to use advances in technology and mobile devices to expand the capabilities of its combat forces. Commercial off-the-shelf (COTS) mobile technology enhances interconnectivity and command & control capabilities to give a competitive advantage to those, including the enemy, who are able to leverage its potential. Mobile devices are recognized as an integral component of the digital interoperability and expeditionary capability emerging to enable the Department of Defense (DOD) to operate in rapidly changing environments. Currently, through the use of a traditional acquisition approach, the USMC is having difficulty in procuring mobile devices before they become obsolete.

B. PROBLEM STATEMENT

The USMC has historically struggled to procure capabilities fast enough to take advantage of technological advances before they become obsolete. In particular, the USMC's operational requirements reflect an increasing demand to procure mobile devices that provide broadband secure capability at low cost and high volume. The ability to take advantage of the newest technological advances as they become available would also aid the USMC in closing the gap between release and operational capability.

This research seeks to identify and assess acquisition strategies to support rapid adoption and integration of emerging COTS mobile devices into the tactical domain. Procurement recommendations will be provided from clearly identifying DOD standards for mobile devices, while analyzing available acquisition architectures through policy and regulation reviews.

C. PURPOSE

The purpose of this research is to determine an acquisition strategy for the USMC that supports the timely procurement of COTS mobile devices for tactical use. Obstacles involving policy and technology will be addressed to gain a better understanding of why current methods are insufficient and what viable solutions are available. This is important because the USMC will be able to leverage the potential uses of mobile devices to enhance operational effectiveness before exceeding its obsolescence life-cycle.

This research will provide a streamlined acquisition option to purchase COTS mobile devices for the USMC using current policies and regulations. A comparison of acquisition programs and our proposed strategy will be conducted to determine the optimal application for the USMC to enable expedient procurement of COTS mobile devices.

D. RESEARCH QUESTIONS

1. Do current acquisition strategies allow for cost effective acquisition of COTS mobile devices, specifically smart phones, before they become obsolete?

2. How can the USMC rapidly procure smart phones while meeting DOD requirements?

E. OBJECTIVES

Current acquisition strategies will be examined to determine their individual feasibility and advantages/disadvantages for procurement. An alternative acquisition strategy will be proposed and compared against those that were examined to offer an alternative to the current strategies.

F. METHODOLOGY

Initial research methods will focus on secondary research targeted at various acquisition projects. Programs, both successful and unsuccessful and of different schedule and performance will be evaluated. Data from multiple Acquisition Category (ACAT) I acquisition programs and types of procurement will be examined that relate as

closely as possible to mobile devices. This data will come from a variety of sources including the Defense Acquisition Management Information Retrieval portal and Acquisition Information Repository. COTS programs procured through both the full acquisition cycle and rapid acquisition organizations will be included. Each project will be evaluated in terms of schedule to determine how well its acquisition strategy was met. Commercial smart phone data, to include several different brands and models, will be researched and obtained to determine cost, schedule and performance metrics.

G. SCOPE

The scope of this research will include traditional and non-traditional acquisition strategies and an examination of rapid acquisition organizations. Device and network architecture, management, and security will be addressed, but will not be studied in depth within this thesis. A revised acquisition strategy will be proposed to allow the rapid acquisition of mobile devices and will include recommendations and operate within the limitations of the current policy and regulations. Specific policy changes will not be proposed in this paper, but will be recommended for analysis for future research.

H. THESIS ORGANIZATION

This thesis is organized into five chapters. Chapter I provides an overview of the problem and explains the methodology and scope of the research. Chapter II gives a comprehensive background review on definitions and concepts discussed within the thesis, to include various rapid acquisition organizations and available procurement methods. Chapter III provides data on the commercial release cycle of COTS mobile hardware and software and certification timelines for mobile devices on Commercial Solutions for Classified (CSfC) devices and the DOD Information Network Approved Products List (DoDIN APL). Chapter IV discusses our proposed acquisition strategy and a comparison of information technology (IT) acquisition strategies. Chapter V states our conclusions and provides our recommended acquisition strategy and areas of future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. INFORMATION TECHNOLOGY TRENDS AND POLICIES

Information technology spans a wide range of systems and devices, and includes both hardware and software. Organizations often struggle to understand how to use IT to best increase the productivity and performance of the organization. Organizations release policy and guidance, often addressing major issues such as security, acquisition and strategy. IT is also always changing, both from a hardware and software perspective, and organizations must be able to adapt and leverage recent advances in both realms to make full use of IT available to them.

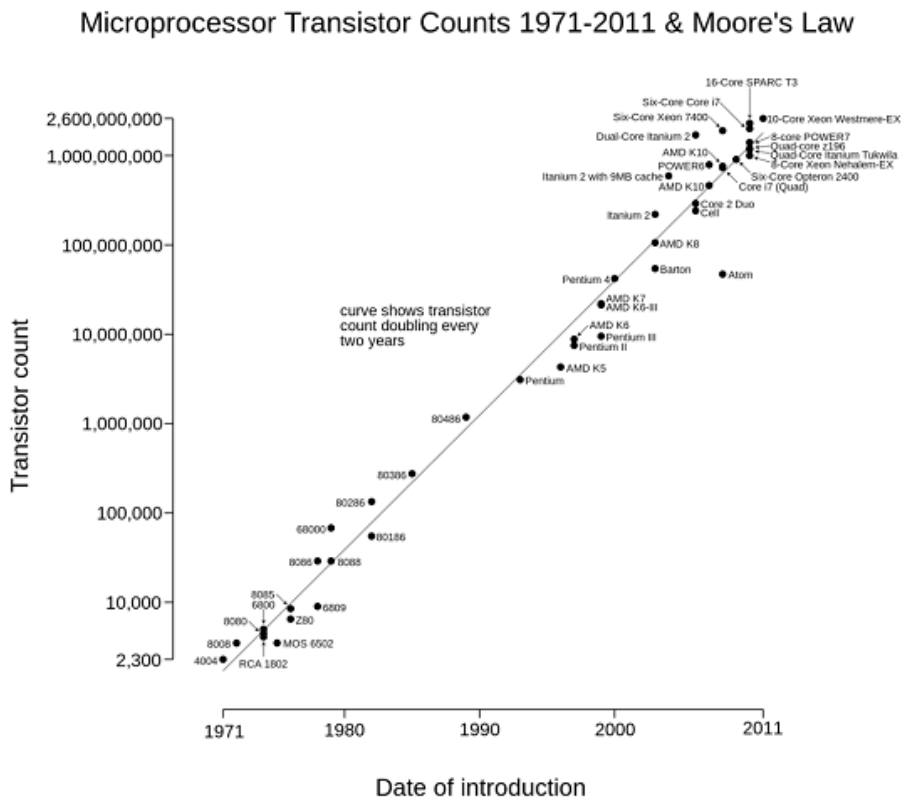
1. Development of Commercial Hardware/Software

Commercial hardware and software has been in development for several decades, and continues to evolve at rapid paces that dictate current technology. Recently, technology, and specifically software, is often evolving at a much more rapid rate than ever before, often causing older "legacy" systems to become obsolete. This section explores the current trends in commercial software and hardware development and how that is affecting current and future technologies.

a. Moore's Law

Gordon E. Moore, co-founder of Intel, correctly predicted in his 1965 article, "Cramming more components onto integrated circuits," that the number of transistors on a circuit per unit area would double approximately every two years. For the past 40 years, this prediction, now known as "Moore's Law," has held true and has led to similar growth rates in many other technological areas (Alastruey, Briz, Ibanez, & Vinals, 2006). The advancement of microprocessors from 1971 to 2011 is shown in Figure 1.

Figure 1. Moore's Law and Transistors from 1971 to 2011.
Source: Davies (2013).



Moore's Law and its implementation have had a profound impact on the electronic components industry, and more specifically the cell phone industry, as manufacturers seek to take advantage of the advances in computing power of the semiconductors and microprocessors used in mobile devices. Generally, a doubling of the transistor count will lead to a proportional increase in processing speed, and ultimately computing power (Alastruey et al., 2006). In addition to computing and processing power, energy efficiency has also increased, allowing devices to be made smaller due to lower power requirements (Intel, 2017). Recently, however, it appears that Moore's Law has begun to lose steam. Instead of the usual 2 years to double capacity and speed, it appears that doubling currently takes approximately 2.7 years (Koomey & Naffziger, 2015). This slowdown, however, has resulted in other innovations and improvements to include energy efficiency (Koomey & Naffziger, 2015), innovation through open source hardware (Huang, 2015), and advances in semiconductor material (Wood, 2008). All of

these advancements are in an effort by companies to continue to meet customer expectations of a doubling of capacity every two years to which the industry has become accustomed the past 40 years.

b. Speed of Mobile Phone Technology Development

Since the introduction of the first cell phone in 1973, and the first commercially available cell phone in 1983, the cell phone industry has seen rapid growth over the past 25 years (Thacker & Wilson, 2015). As of 2015, cell phone technology was so widely used that 30% of households in the United States were cell phone only and lacked a traditional land line (Macher, Mayo, Ukhaneva, & Woroch, 2013). Companies seek to match consumer demand for new hardware and software as quickly as economically feasible to ensure they remain profitable. Technological progress and innovations developed by firms are often easily copied by competitors due to their availability to all operators (Thacker & Wilson, 2015). This leads to innovative ideas and technologies being rapidly adopted by almost all cell phone manufacturers in short periods of time. Quick development of new products is deemed economical, and it is encouraged because it minimizes overall development costs through efficient use of resources and enables firms to experience higher profitability and market share (Lin, Huang, & Chan, 2012).

While smart phones have a life expectancy of around 4.7 years, according to a study by the Consumer Electronics Association, actual smart phone release dates correspond more closely to a 2-year period (Ely, 2014). This 2-year release schedule matches most 2-year service plans given by cell phone service providers such as Verizon, AT&T, Sprint, and T-Mobile that have become popular with consumers. Mobile phone features have also been evolving at much the same pace as the actual hardware. Text messaging, through SMS, was introduced in the late 1990s, video games in 1997, and the first wireless application protocol allowing users to access web pages in 1999 (Giachetti & Marchi, 2010). A summary table of examples of such technology and their introduction is presented in Figure 2.

Figure 2. Mobile Product Technology Introductions.
Source: Giachetti and Marchi (2010).

Product technology	Firms introducing the technology*	Year of introduction
Second half of the 1990s		
Voice dial	Philips	1997
Composer	Ericsson	1997
Infrared	Nokia	1997
Games	Nokia	1997
Downloadable ring	Nokia	1998
Email client	Nokia	1998
WAP	Nokia	1999
First half of the 2000s		
Polyphonic ringtone	Panasonic	2000
SMS chat	Nokia	2000
MP3	Samsung and Siemens	2000
Bluetooth	Ericsson	2001
Colour screen	Nokia and Ericsson**	2001
MMS	Motorola	2002
Photocam	Sharp	2001
Videocam	Nec	2003
Wi-Fi	Motorola	2004
Second half of the 2000s		
iTunes	Motorola	2005
GPS	Samsung	2007

Notes: *The first firm adopting the new product technology in its portfolio.
**A couple of phone models capable of displaying only four colours were introduced by Siemens in 1997. However, the first phones capable of displaying a complete range of colours (more than 200 colours) were introduced in 2001 by Ericsson and Nokia.

c. Obsolescence

Obsolescence from a technology standpoint is nothing new, and can take on many different forms. Planned obsolescence is a designer and/or manufacturer approach that calls for product designs with artificially reduced life cycles (Seland, 2015). This planned obsolescence is often motivated by the desire to increase sales or shorten the time to product replacement. Obsolescence is not unique to the technology sector, affecting almost every industry (Jennings, Wu, & Terpenny, 2016). Semi-conductors, the heart of most electronic devices generally only have an average lifespan of approximately three years from introduction to End-of-Life announcement (Karalias, 2010)

Generally, a technology or product is considered obsolete when it is no longer being manufactured (Ward & Sohns, 2011). This decision to cease manufacturing corresponds to a loss in value, as perceived by the consumer, resulting from a loss of utility of the product (Rai & Terpenny, 2008). This loss in value is manifested by the emergence of a more cost-effective alternative, one that can achieve better performance (as defined by the user), one that is deemed to be higher quality, or any combination of the three (Jennings et al., 2016). A product may be technically obsolete, but can still be functioning as intended after production has ceased. Smart phones, such as the iPhone and Droid, are prime examples; new versions constantly being released, but users continue operating older devices with much the same capability.

2. Mobile Device Defined

The definition of mobile device varies from organization to organization, due to the fact that mobile devices encompass many different platforms and have evolved rapidly over the last several years. In addition to mobile devices, common terms such as tablets, cell phones and personnel electronic devices are often used interchangeably with mobile devices. Various definitions of a mobile device as given by many different organizations within and outside the DOD are presented in Table 1.

Table 1. Definitions of Mobile Devices

Name	Organization	Document (Year)	Definition
Mobile device	CIO Council	Government Mobile and Wireless Security Baseline (2013b)	Mobile devices include smartphones and tablet computers that support multiple wireless network connectivity options (primarily cellular and Wi-Fi), and host voice and data applications. The devices run mobile operating systems which are used to access mobile sensors, data and voice services.
Commercial Mobile Device	DOD CIO	DOD Commercial Mobile Device (CMD) Interim Policy (2012)	A subset of portable electronic devices (PED) as defined in DoDD 8100.02 that provide one or more commercial wireless interfaces along with a compact user input interface (Touch Screen, Miniature Keyboard, etc.) and exclude PEDs running a multi-use operating system (Windows OS, Mac OS, etc.). This definition includes, but is not limited to smart phones, tablets, and e-readers.
Portable Electronic Device	DOD	DoDD 8100.02, Use of Commercial Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG) (2007)	Any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to PDAs, cellular/PCS phones, two-way pagers, email devices, audio/video recording devices, and hand-held/laptop computers.
Smart Phone	NIST	Smart Phone Tool Specification (2010)	A full-featured mobile phone that provides users with personal computer like functionality by incorporating PIM applications, enhanced Internet connectivity and email operating over an Operating System supported by accelerated processing and larger storage capacity compared with present cellular phones.

Table 1 cont'd. Definitions of Mobile Devices

Name	Organization	Document (Year)	Definition
Cell Phone	NIST	Smart Phone Tool Specification (2010)	A device whose major function is primarily handling incoming/outgoing phone calls over a wireless network (e.g., GSM, CDMA) with limited task management applications.
Mobile Device	NIST	Guidelines for Managing the Security of Mobile Devices in the Enterprise (2013)	Small form factor. Wireless network interface (Wi-Fi, cellular networking, etc.). Local built-in (non-removable) storage. OS that is not a full-fledged desktop or laptop OS. Applications available through multiple methods.
Portable Electronic Device	U.S. Army	Army Regulation 25–2, Information Assurance (2007)	Portable ISs or devices with or without the capability of wireless or LAN connectivity. These include, but are not limited to, cell phones, pagers, personal digital assistants (PDAs) (for example, Palm Pilots, Pocket PCs), laptops, memory sticks, thumb drives, and two-way radios. Current technologies (infrared, radio frequency, voice, video, microwave) allow the inclusion of numerous capabilities within a single device and dramatically increases the risks associated with IS and network access
Portable Electronic Device	USMC	HQMC Implementation of USMC Enterprise Cybersecurity Directive 005 Portable Electronic Devices (2014)	Government provisioned, privately purchased and contractor provided laptops, pocket PCs, personal digital assistants, tablets, MP3 players, cell phones, video cameras, BlackBerry devices and pagers.

3. Government Strategy and Guidance

Government strategy and guidance dictate the paths that various agencies and organizations take. Recognizing the advantages that mobile devices can provide, the Federal government and DOD have implemented and produced many different types of policy and guidance that relate to mobile device use. These policies range from and include overarching strategy goals, IT guidance and regulations and cybersecurity concerns.

a. Digital Government Strategy

The Digital Government Strategy (DGS) sets out to accomplish three goals: 1) Enable the American people and workforce, which is becoming more mobile, to access government information at anytime, anywhere, on any device, 2) Ensure the government seizes the opportunity and benefits of managing and procuring devices in secure and affordable ways, 3) Unlock government data to enable an innovation spur and increase the quality of services offered to the American people (White House, 2013).

The DGS also seeks a goal of developing a shared mobile application development program to enable secure, device-agnostic applications with an additional goal of streamlining application development through cross agency collaboration. For procurement, the government should focus on an enterprise-wide asset management strategy to effectively leverage buying power, both from a device and service perspective. The DGS directs that agencies will be required to enable two customer priority services to be accessed using mobile devices and to prioritize which services that are currently being provided can be optimized for mobile use.

b. The Department of Defense Strategy for Implementing the Joint Information Environment

The Joint Information Environment (JIE) seeks to ensure DOD stakeholders have access to information and data to support decision making through secure, reliable and agile means (Department of Defense [DOD], 2013). Achieving this access to information will be provided by a multitude of devices, including incorporating the ideas of mobility and enterprise services. The DOD recognizes the advantages that mobility services, such

as mobile devices and portable cloud enabled C2 systems, and seeks to provide both unclassified and classified mobility services in support of the JIE. The use of thin-client and desktop virtualization is highlighted as providing access to users' computer environment, particularly through the use of mobile devices because of their ease of use and portability. Security is addressed through a Single Security Architecture, with the goal of providing the DOD with a common network security architecture to include support for non-traditional users such as mobile users.

c. DOD IT Enterprise Strategy Roadmap

The DOD IT Enterprise Strategy Roadmap identifies that in the past, DOD IT projects have been undertaken with an individual project goal in mind (DOD, 2011). Going forward, the goal is to consolidate the IT infrastructure to achieve better operational capability and cost savings. Users should have access to timely information across the DOD Information Enterprise, including from mobile devices. The network infrastructure upgrades should produce an environment that is secure, resilient, and restorable, necessary for users operating in increasingly mobile environments. The DOD also seeks to leverage existing and future advances in the types of devices that users use to obtain their information.

d. DoDD 8000.01

While not specific to mobile devices, DoDD 8000.01, Management of the Department of Defense Information Enterprise (DOD IE) does give several criteria for managing investments in "information solutions" (DOD, 2016). These include using performance/results to evaluate systems, review all IT investments for compliance with architectures, standards and policies, evaluate life-cycle management and assess and mitigate risks. Ideally, IT will be developed in useful increments that have a defined scope and duration, solve a problem, deliver a capability, and provide a tangible benefit that is independent of future increments (DOD, 2016).

e. Marine Corps Information Enterprise Strategy Implementation Planning Guidance Version 1.1

The Marine Corps wishes to modernize their IT assets and services to provide next-generation capabilities in support of the Marine Corps Enterprise Network (MCEN) (USMC, 2013b). Strategic Objective 4 of the document recognizes the need for incorporating emerging IT and Command, Control, Communication, Computers and Intelligence (C4I) technologies into the MCEN. This applies to both GOTS and COTS software/hardware. The need for end-user devices, in coordination with the USMC CMD Strategy, must be developed to provide affordable, COTS, non-proprietary items to support the warfighter. The technical implementation of the USMC CMD Strategy through development of security, policy and technical capabilities is also mandated (USMC, 2013b).

4. Government Adoption and Use of Mobile Devices

Government agencies, to include the DOD have been keen to take interest in integrating mobile devices into their communities to leverage the many benefits mobile devices provide. This section will explore the various current policies and guidance put out by several government agencies (Federal, State, DOD, etc.) in relation to current usage of mobile devices within several agencies.

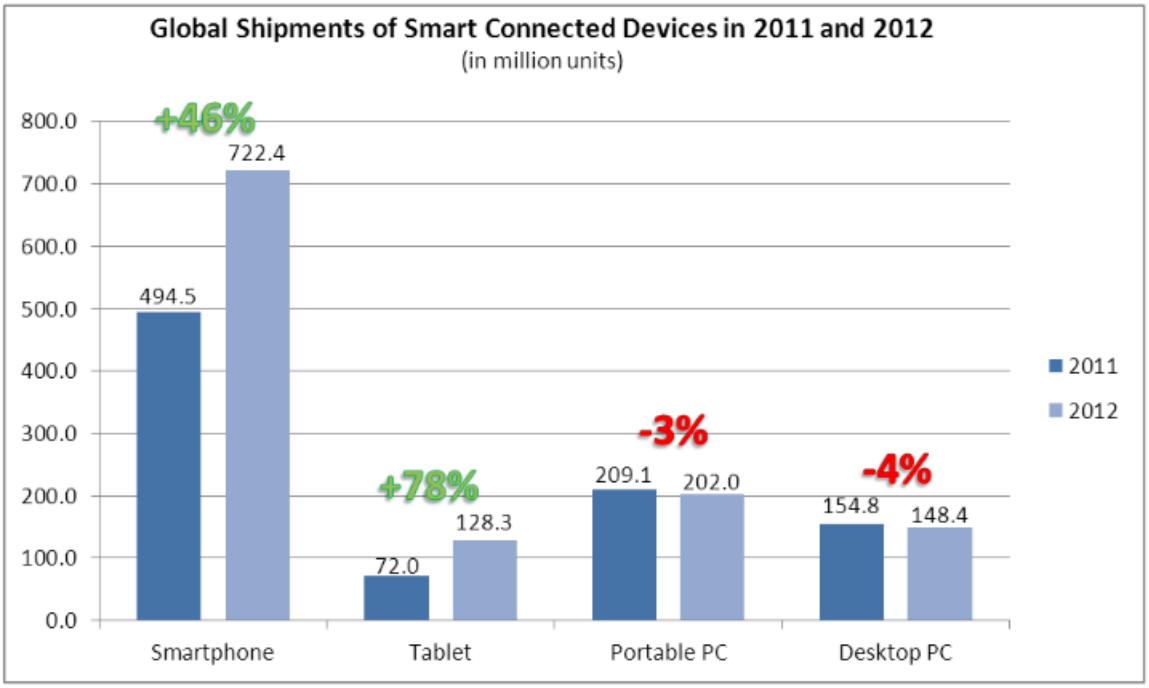
a. Adoption of Commercial Mobile Applications within the Federal Government

This policy focuses specifically on the goal of developing the secure delivery and use of commercial mobile applications into the Federal government, as outlined in the Digital Government Strategy Goal 5.4 (Chief Information Officer [CIO] Council, 2013a). The use of BYOD and use of commercial mobile applications is not covered in this document, and is covered in a separate policy. The study finds that several agencies have already employed commercial mobile applications (ranging in number from 5–20) for specific users.

By allowing access to commercial mobile applications on government-furnished equipment, employees gain the advantage of being able to access work-related

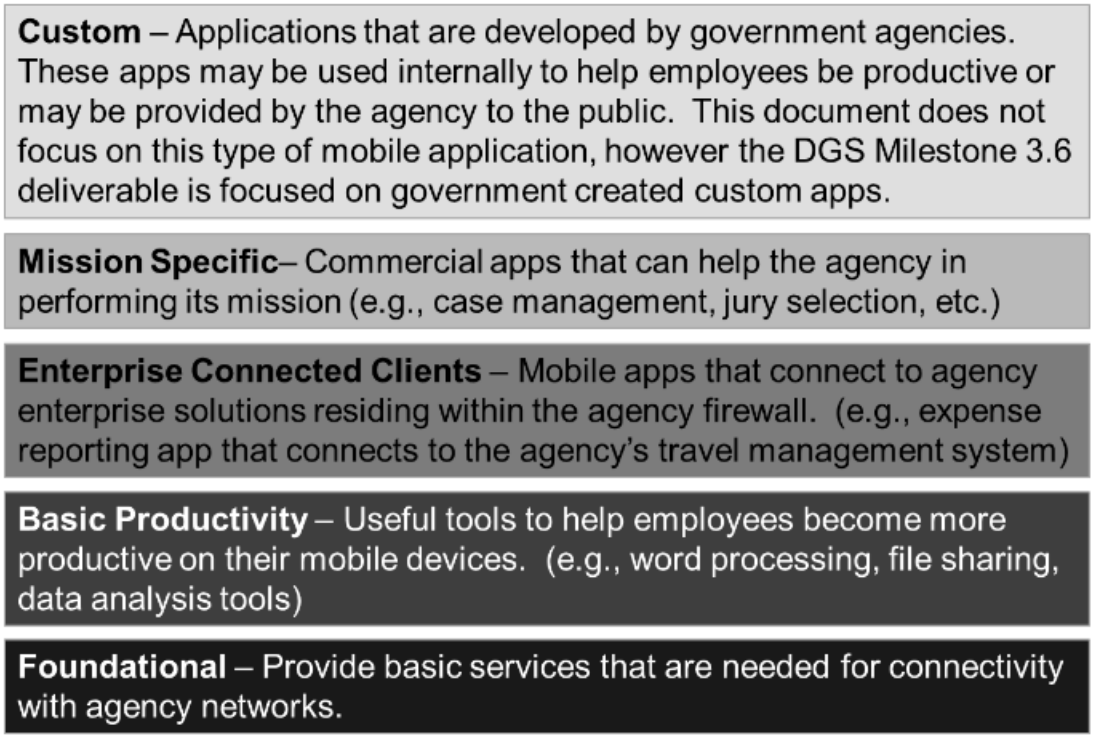
information and perform work-related tasks with government furnished mobile devices. Mobile devices are also often less expensive and easier to install compared to traditional desktop applications, leading to cost savings and efficiencies within organizations. The government seeks to mimic the use of COTS hardware and software in the desktop realm, and apply this model to mobile applications and hardware through the use of existing applications and mobile platforms (Apple, Android, BlackBerry, etc.) The adoption rates of mobile devices (cell phones and tablets), compared to portable and desktop PCs, can be seen in Figure 3.

Figure 3. Smart Connected Devices Sales Growth/Decline, 2011 vs. 2012. Source: CIO Council (2013a).



Surveys from 20 different government agencies revealed that applications could be divided into five main categories: foundational, basic productivity, Enterprise connected clients, mission specific and custom (CIO Council, 2013a). Specific definitions for such applications can be seen in Figure 4.

Figure 4. Definition of Different Types of Commercial Applications. Source: CIO Council (2013a).



The survey found that basic productivity and foundational applications accounted for almost 90% of application usage and downloads among the agencies. Common challenges were also identified and included fraudulent applications, malware, inappropriate applications, and excessive use of network resources in bandwidth restricted environments. Frequent updates were also cited as a difficulty, due to increased security concerns and public cloud concerns were also highlighted due to confusion on how to deal with government information that is located on a public cloud (from both a privacy and security concern).

Identifying risks in the usage of mobile apps also revealed a distinct conflict of interest between user flexibility and organizational control. This risk model applies to a multitude of subjects including procurement, review and approval, discovery, distribution/installation and management and support. The report recommends a government wide commercial application catalog that supports approved applications and a description of their intended use and other characteristics. A need for a government

wide Terms of Service for applications is recommended to enable the approval and accreditation for applications within differing agencies to be expedited and reduce overlap.

b. Government Use of Mobile Technology: Barriers, Opportunities and Gap Analysis

With the release of the Digital Government Strategy, the Federal Chief Information Officer (CIO) Council chartered a team to explore the barriers, opportunities, and gap analysis with the current use of mobile technology with the U.S. government (CIO Council, 2012b). This team identified four different types of users (employees, executives, partners, and the public) and conducted surveys to determine mobile use across 21 federal agencies. Feedback determined that CIOs focused on three main categories: capabilities, cost, and security.

While capabilities exist on individual mobile devices, agencies were key to identification of the capabilities issues with mobile device management (MDM) and the interoperability and interconnectivity of BYOD vs. GOTS vs. COTS devices and architectures. The largest cost barrier was the lack of a government wide contract for both mobile device hardware (cell phones, tablets, etc.) and services/data plans. Several agencies expressed they were well into the acquisition process for various hardware and services, and could not afford to wait for a government-wide procurement system. Rapidly changing technologies and maturity of hardware devices was seen as a benefit, but also brought cost issues when paired with the relatively slow and immature support infrastructure products. From a security perspective, limited options related to strong authentication and encryption and their slower development rate than hardware was addressed. Specifically, there exist few validated encryption models and methods for classified/sensitive information and this limits the operational effectiveness for many agencies. Future encryption models are often slow to be implemented and certification and validation is often even less timely. Lack of uniformity across hardware and operating systems also poses a challenge and often contradicts a BYOD and device agnostic approach to MDM.

The report seeks to address these problems by suggesting several solutions. Policy and regulation overlap should be kept to a minimum, and should support the more widespread use of mobile devices in the government workforce. A cross-functional team should be established to reach conclusions and legal decisions on many of the issues that have been previously identified. Government agencies should also look beyond the initial capability that mobile devices and applications provide to achieve continued effectiveness in the long term.

c. Bring Your Own Device

A BYOD policy was published in response to the Digital Governance Strategy dictating the publication of guidance regarding BYOD programs for Federal agencies seeking to implement such programs themselves (CIO Council, 2012b). Evaluation of several agencies, including the Alcohol and Tobacco Tax Trade Bureau (ATTTB), State of Delaware and U.S. Equal Employment Opportunity Council (EEOC), who had implemented BYOD programs were evaluated and results compiled.

ATTTB sought to reduce the costs associated with installing and refreshing software on both desktop and laptop computers used for everyday tasks. ATTTB recognized its workforce was highly mobile, with a large percentage of the workforce telecommuting and sought to provide access through thin client computing devices. This allowed users access using their own laptops and desktops using the thin client, with no data ever touching the end user device.

The U.S. EEOC implemented its BYOD program in response to a 15% IT budget cut. By allowing users to install third-party software onto their devices which allowed the agency to control security settings, the U.S. EEOC hoped to entice users away from using their BlackBerry device and eventually transition away from BlackBerry use altogether. The U.S. EEOC did not offer to pay for users completely transitioning over to 100% BYOD, and required users to pay for all government voice and data usage.

The State of Delaware opted to implement a BYOD program because its current state-provided BlackBerry devices were reaching the end of their life and would require a life cycle replacement. Unlike the EEOC, Delaware did provide a flat reimbursement for

BYOD use to state employees whose job duties were deemed to require the frequent use of cell phone or email access. This reduced Delaware's expenditure on wireless costs by 15% and costs in procuring devices of 45%.

d. DOD Mobile Device Strategy

The purpose of the DOD Mobile Device Strategy is to identify goals and objectives to be able to fully utilize and capitalize on the advantages and capabilities that mobile devices provide (Department of Defense Chief Information Officer [DOD CIO], 2012a). The policy sets three overarching goals with a subset of objectives within each goal spelled out in Table 2:

Table 2. DOD Mobile Device Strategy Goals and Objectives.
Source: DOD CIO (2012a).

Goal	Objective
1. Advance and Evolve the DOD Information Enterprise Infrastructure to Support Mobile Devices	1. Evolve Spectrum management
	2. Expand infrastructure to support wireless capabilities
	3. Establish a mobile device security architecture
2. Institute Mobile Device Policies and Standards	1. Develop mobile device policy and standards
	2. Establish a mobile device management service
	3. Educate and train mobile device users
3. Promote the Development and Use of DOD Mobile and Web-Enabled Applications	1. Establish a common mobile application development framework
	2. Institute a mobile application certification process
	3. Provide an enterprise mobile application environment
	4. "Web-enabled" IT capabilities for mobile device support

It recognizes that from a DOD perspective, mobile users span a wide range to include office/garrison environments as well as tactical environments. Three different types of users are defined: enterprise-wide, tactical and executive. At the conclusion, a

need for an implementation plan was recognized with a goal of evaluating the strategy based on a small initial population of users.

e. DOD Commercial Mobile Device Interim Policy

Separated into three distinct parts, the DOD Commercial Mobile Device Interim Policy seeks to provide guidance on BlackBerry security features, clarify the use of non-enterprise CMDs and establish guidelines for support of CMD applications (DOD CIO, 2012b). With the increased need for Apple/Android devices and applications, the DOD published this guidance to enable BlackBerry users some leeway in security settings to enable requirements to be met with current BlackBerry models. The goal was to reduce the need to purchase standalone Apple/Android devices by allowing DOD COCOMs and agencies/departments to modify optional security settings according to the BlackBerry Security Technical Implementation Guide. After assessing risk, and making a determination, security settings can be changed based on operational needs to enable functionalities including camera/video recordings, Global Positioning System (GPS), social networking, etc. (DOD CIO, 2012b).

The second portion of the policy clarifies the use of non-enterprise connected CMDs in the DOD. Again, COCOMs and agencies/components are allowed to use CMDs for non-sensitive information and when not connected to the enterprise. This enables the use of CMDs for tasks including map reading/viewing, recruiting activities and user training (DOD CIO, 2012b).

CMD applications are identified as potentially enhancing user productivity but also produce security and interoperability issues. Applications must meet current DOD policy in regards to security, which the policy states Defense Information Systems Agency (DISA) will provide the DOD CIO. DISA will also maintain all CMD applications on a central website (DOD CIO, 2012b).

f. DOD Commercial Mobile Device Implementation Plan

Released shortly after the DOD Mobile Device Strategy memo, the DOD Commercial Mobile Device Implementation Plan seeks to identify a phased approach to

introducing non-tactical mobile applications within the DOD enterprise (DOD CIO, 2013). It also updates the DOD Mobile Device Strategy to include the distinction and inclusion of secure classified and protected unclassified mobile solutions using COTS devices and capabilities. Classified solutions are directed to use the National Security Agency (NSA) Commercial Solutions for Classified (CSfC) process (DOD CIO, 2013).

The DOD recognizes the capability gaps that were identified during the JROC Capability Gap Assessment and collaboration with Office of the Secretary of Defense (OSD) and seeks to fill or mitigate some of those gaps using wireless network services, approved mobile devices and applications management. MDM plans are identified as one of the key factors for ensuring unified success, and include a vision for a Mobile Application Store (MAS) that works hand in hand with the MDM plan to allow users access to differing applications (DOD CIO, 2013).

Procurement of mobile devices will be accomplished through a combination of DISA, DOD Components and GSA, based upon validated requirements and supported by business and cost analysis. The GSA is referenced in relation to the Digital Governance Strategy, and directs DOD agencies to contract with GSA once GSA is able to procure mobility services that meet DOD requirements. The DOD also seeks to support multi-vendor procurements to ensure a device agnostic approach (DOD CIO, 2013).

The DOD CIO is established as the final authority for enterprise wide mobility solutions, and DOD members will participate in a Commercial Mobile Device Working Group (CMDWG). The purpose of the CMDWG is to approve all policy, standards and processes related to mobile devices and mobile device management. It directs DOD components to establish their own MDM service to support users specific to that service, and includes the requirement that service level mobile devices and MDM must meet current DOD level requirements (DOD CIO, 2013).

g. Marine Corps Commercial Mobile Device Strategy

The USMC has seen a significant increase in demand for the use of mobile devices for a variety of reasons including ease of use, mobility and increased productivity (USMC, 2013a). As of 2013, the use of mobile devices on MCEN was limited to

privileged users who are defined as an individual who the command as mission critical or mission essential and therefore provided with a government furnished mobile device or reimbursed for use of their own personal mobile device. The Marine Corps seeks to acquire mobile devices based on identified needs and user requirements. By validating requirements and needs, trends in the civilian sector that result in acquiring technology that does not often match a need or provide a significant enough increase in capability can be avoided. The USMC CMD Strategy is broken down into four main goals, each with a subset of objectives as outlined in Table 3.

Table 3. USMC CMD Strategy Goals and Objectives.
Source: USMC (2013a).

Goal	**Objective**
1. Establish a Secure Mobile Framework (SMF)	1. Develop Mobile Device Policy
	2. Expedite Procurement
	3. Advance Secure Mobile Devices
	4. Develop Secure Mobile Applications
	5. Standardize Testing
	6. Expand Secure Infrastructure
	7. Certification and Accreditation
	8. Optimize Operations
2. Transition the Unclassified Mobile Device Infrastructure to a Cost Effective and Platform Agnostic Environment	1. Continue Current Mobility Operations and Maintenance Support
	2. Identify Mobile Solutions which Support Platform Agnostic Devices
	3. Mandate and Promote the Use of Telecommunication Expense Management Solutions
3. Collaborate with DOD and Industry Partners to Develop a Classified Mobile Device Capability	1. Coordinate with Other Services
	2. Leverage Existing Technologies
4. Incorporate Personally Owned Mobile Devices	1. Develop Personally Owned Mobile Device Policy
	2. Develop Procedures to Identify Authorized Personally Owned Mobile Devices
	3. Standardize Security Control Procedures
	4. Privileged Users and Non-Privileged Users

Marine Corps participation within the DOD CIO CMDWD will continue, along with the Department of the Navy (DON) Enterprise Mobility Integrated Product Team in order to coordinate CMD strategy and vision. Doing so will help the Marine Corps avoid duplication of effort and identify best value options for equipping the warfighter.

5. Security and Interoperability Requirements of Mobile Devices

The DOD has strict requirements when it comes to IT devices operating on the DOD network. Strict security requirements must be adhered to depending on how the devices are being used and what types of data is being stored and transmitted. IT systems and devices must also be able to operate with other systems in order to leverage advantages provided by using multiple systems and sharing of data and information.

a. DoDI 8330.01: Interoperability of Information Technology, Including National Security Systems

DoDI 8330.01 lays out the requirements for interoperability among IT within the DOD (Department of Defense [DOD], 2014a). IT is required to interoperate with existing and planned systems within DOD and extends to other U.S. government agencies and departments as well. Specific IT interoperability and supportability shall be defined through the Defense Acquisition System (DAS), Joint Capabilities Integration Development System (JCIDS) and Doctrine, Organization, Training, Materiel, Leadership, Personnel and Facilities (DOTMLPF) construct. While seeking to maximize interoperability, cybersecurity concerns must also be balanced in a risk based approach. The directive also establishes testing procedures that all IT devices must adhere to in order to satisfy the Net Ready Key Performance Parameter (KPP) requirements and ultimately be granted approval to operate on a DOD network. The Joint Interoperability Test Command (JITC) was given the responsibility for ensuring that IT devices meet the Net Ready KPP standard and are responsible for ensuring testing meets DOD standards.

b. DoDI 8420.01: Commercial WLAN Devices, Systems and Technology

This policy directs that wireless devices, including portable electronic devices (PED) such as cell phones, when connected or integrated with the Global Information

Grid (GIG) comply with several other policies including DoDI 8500.01 and be certified/accredited with DoDI 5200.40 (DOD, 2009). DoDI 8420.01 also separates data at rest, which must meet separate Federal Information Processing Standard (FIPS) 140–2 requirements. Devices transmitting or storing classified information must be approved by the appropriate Designated Approving Authority and use NSA-approved encryption. The policy also forbids the use of PEDs while operating using a wired connection and a wireless connection (DOD, 2009).

In reference to mobile devices, this instruction classifies any type of PED that uses IEEE 802.11 connectivity as a Wireless Local Area Network (WLAN)-enabled PED that must adhere to the instruction (DOD, 2009). The instruction specifies it does not apply to other types of connectivity, including but not limited to 3/4G cellular, Bluetooth, WiMAX, Near Field Communication (NFC), etc. Security requirements, along with management criteria are separated for both classified and unclassified systems and devices.

c. DoDI 8100.04: DOD Unified Capabilities

This policy addresses the integration of the numerous network and IT components to provide a UC to the DOD for all future and current systems (DOD, 2010). It identifies the responsible parties for DOD interoperability testing (JITC) and information assurance (DOD CIO). The UC Approved Products List, which is discussed later, is created to ensure a one-stop shop for all IT devices that are allowed to operate on the DOD network.

d. DoDI 8500.01: Cybersecurity

This instruction provides the basis and overarching guidance for all things related to cyber security for all DOD IT systems and data stored electronically (DOD, 2014b). Classified data and systems, and specifically Sensitive Compartmentalized Information (SCI), is addressed and the Director of National Intelligence is identified as being the leading authority for most classified systems. Overall, the DOD seeks to leverage systems to perform functions and provide capabilities based on a cybersecurity risk assessment framework, balancing operational and realistic needs with cybersecurity. DOD IT

systems will undergo rigorous testing and certification to ensure they meet standards set forth for their functions and adhere to the cybersecurity risk based approach model. Overall the goal is to ensure DOD IT systems provide reasonable safe and secure capabilities that enhance the DOD effectiveness.

B. GOTS, COTS, AND COMMERCIAL ITEMS

Although GOTS provide customizable solutions through proprietary hardware/software, commercial items and COTS enable higher speeds, lower costs, and more adaptability. As a part of a RAND study, Gompert (1999) stated "The U.S. military market now makes up just 2 percent of the demand for IT in the United States (U.S.), down from 25 percent in 1975" (p. 52). The research and development (R&D) gap between the U.S. military and the commercial sector has continued to widen ever since. "In global terms, civilian R&D is about 10 times as large as military R&D" (Brzoska, 2006, p. 1). There is increasing trend toward the leveraging of commercial technology for military purposes. Agre, Gordon, and Vassiliou (2013) offered a few advantages to COTS that may explain this trend: "1) advanced features and functions, 2) faster time to market, 3) less cost, 4) less R&D for the government, and 5) reduced size, weight, and power compared with similar military systems" (p. 1). Limitations to commercial adoption may include multiple considerations: 1) technical such as robustness and security, 2) environmental such as survivability, lack of fixed infrastructure, high mobility, and ruggedness, and 3) acquisition such as regulations and processes (Agre et al., 2013). Agre et al. (2013) suggested that direct adoption of COTS products at the tactical edge may not be feasible and instead, modifying COTS products to enable modularity will allow "the ability to evolve with the market-drive commercial evolution of the device" (p. 1). Although Agre et al. preferred the modification of COTS, there may be some confusion as to how much a COTS product may be modified before it is considered a commercial item.

Defining what are commercial items and COTS is important in using a shared vocabulary for the rest of the thesis as well as our understanding of the problem in acquiring mobile devices. Defense Logistics Agency (DLA) (2010) defined a commercial

item as “any product or service that is customarily used by the general public or nongovernmental entities for nongovernmental purposes” (p. 3). Relevant criteria include: 1) “Products, other than real property, that have been offered for sale, lease, or license to the general public”; 2) “Products that evolved through advances in technology or performance and will be available in the commercial market in time to meet the delivery requirements of the solicitation”; 3) “Products that have received minor modifications to meet DOD requirements”; and 4) “Products that were created by integrating commercial subsystems and components into a unique system” (Defense Logistics Agency [DLA], 2010, p. 3). A minor modification of a commercial item does not considerably change the nongovernmental function, essential physical characteristics, or purpose (DLA, 2010). OSD (2000) defined COTS as

> One that is sold, leased, or licensed to the general public; offered by a vendor trying to profit from it; supported and evolved by the vendor who retains the intellectual property rights; available in multiple, identical copies; and used without modification of the internals (p. 3).

COTS is a more restricted definition of a commercial item with the main difference being that COTS does not allow for internal modification. The DOD trend towards commercial items involves a paradigm switch from the commercial market adapting to DOD requirements to DOD requirements adapting to capabilities available in the marketplace (Office of the Secretary of Defense [OSD], 2000). A commercial-based system must involve adopting original characteristics and functionality of the commercial item and common commercial business practices, while closing the gap between DOD and commercial use (OSD, 2000).

C. GOVERNMENT ACQUISITION METHODS

There are multiple avenues within the federal government to acquire and procure products and services, including new rapid acquisition units and additional authorizations established within the last few years. Exploring both common and uncommon avenues to procurement is important in finding an optimal acquisition strategy. In this section, we will discuss traditional acquisition and procurement methods such as the DAS, General Services Agency (GSA), tools used by program managers and authorized agencies such

as Small Business Innovation Research (SBIR), and unique rapid acquisition units, such as Rapid Capabilities Office (RCO), Defense Advanced Research Projects Agency (DARPA), In-Q-Tel, and Defense Innovation Unit Experimentation (DIUx).

1. Defense Acquisition System

The DOD has three primary decision-making support systems: the Planning, Programming, Budgeting and Execution (PPBE) Process, JCIDS, and DAS (Defense Acquisition University [DAU], 2013). DOD Directive 5000.01 defined DAS as "the management process by which the Department of Defense provides effective, affordable, and timely systems to the users" (Under Secretary of Defense for Acquisition, Technology, & Logistics [USD(AT&L)], 2007, p. 4). An acquisition program is managed by the program manager (PM), who accomplishes program objectives and is responsible to the milestone decision authority (MDA), who has overall authority over the acquisition program (USD(AT&L), 2007). Throughout the acquisition process, the MDA will review the program and make approvals at key decisions points (USD(AT&L), 2017). DOD Instruction 5000.02 (2017) lists the following steps in the process: 1) The DAS begins with the Material Development Decision (MDD) to enter into the Material Solutions Analysis (MSA) phase and determine if a new product is required and to explore alternative solutions; 2) The Risk Reduction Decision (RDD) provides entry into the Technology Maturation & Risk Reduction (TMRR) phase and makes "an investment decision to pursue specific product or design concepts" as well as maturing the technology to a benchmark of Technology Readiness Level (TRL) 6 (see Table 4) or reducing risk; 3) The Engineering & Manufacturing Development (EMD) phase contains three decision points: Capabilities Development Document (CDD) Validation Decision, Request for Proposal (RFP) Release Decision Point, and "a decision to award the contract(s) for development" called Milestone B where the acquisition program becomes a program of record upon approval within the designated ACAT level (see Table 5); 4) The Production & Deployment (P&D) phase contains two decision points: Low-Rate Initial Production (LRIP) called Milestone C and Full-Rate Production (FRP) or the Full Deployment Decision (FDD) and is also when Initial Operational Capability (IOC) is achieved; 5) The Operations & Support (O&S) phase executes the Sustainment of the

product throughout its life cycle and its eventual Disposal and is also when Full Operational Capability (FOC) is achieved (p. 8).

Due to the complexity of the DAS and the uniqueness of each product and circumstances, “MDAs have full latitude to tailor programs in the most effective and efficient structure possible, to include eliminating phases and combining or eliminating milestones and decision points, unless constrained by statute” (USD(AT&L), 2017, p. 9). The DAS is regulated by both statutory and regulatory requirements where statutory requirements must be complied with unless the statute states otherwise, therefore MDAs can primarily tailor regulatory requirements while taking into account “sound business practices and the risks associated with the product being acquired” (USD(AT&L), 2017, p. 2).

Table 4. Technology Readiness Level (TRL) Descriptions. Source: DAU (2017).

Technology Readiness Level	**Description**
1. Basic principles observed and reported.	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology’s basic properties.
2. Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
3. Analytical and experimental critical function and/or characteristic proof of concept.	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
4. Component and/or breadboard validation in laboratory environment.	Basic technological components are integrated to establish that they will work together. This is relatively “low fidelity” compared to the eventual system. Examples include integration of “ad hoc” hardware in the laboratory.

Table 4 cont'd. Technology Readiness Level (TRL) Descriptions. Source: DAU (2017).

Technology Readiness Level	Description
5. Component and/or breadboard validation in relevant environment.	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so it can be tested in a simulated environment. Examples include "high fidelity" laboratory integration of components.
6. System/subsystem model or prototype demonstration in a relevant environment.	Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in simulated operational environment.
7. System prototype demonstration in an operational environment.	Prototype near, or at, planned operational system. Represents a major step up from TRL 6, requiring demonstration of an actual system prototype in an operational environment such as an aircraft, vehicle, or space. Examples include testing the prototype in a test bed aircraft.
8. Actual system completed and qualified through test and demonstration.	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.
9. Actual system proven through successful mission operations.	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.

Table 5. Description and Decision Authority for ACAT I–IV Programs.
Source: USD(AT&L) (2013).

ACAT	Reason for ACAT Designation	Decision Authority
ACAT I	• MDAP (10 U.S.C. 2430) o Dollar value for all increments of the program: estimated by the DAE to require an eventual total expenditure for research, development, and test and evaluation (RDT&E) of more than $480 million in Fiscal Year (FY) 2014 constant dollars or, for procurement, of more than $2.79 billion in FY 2014 constant dollars o MDA designation • MDA designation as special interest	ACAT ID: DAE or as delegated ACAT IC: Head of the DOD Component or, if delegated, the CAE
ACAT IA	• MAIS (10 U.S.C. 2445a): A DOD acquisition program for an Automated Information System (AIS) (either as a product or a service) that is either: o Designated by the MDA as a MAIS program; or o Estimated to exceed: - $40 million in FY 2014 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, deployment, and sustainment, and incurred in any single fiscal year; or - $165 million in FY 2014 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, and deployment, and incurred from the beginning of the Materiel Solution Analysis Phase through deployment at all sites; or - $520 million in FY 2014 constant dollars for all expenditures, for all increments, regardless of the appropriation or fund source, directly related to the AIS definition, design, development, deployment, operations and maintenance, and incurred from the beginning of the Materiel Solution Analysis Phase through sustainment for the estimated useful life of the system. • MDA designation as special interest	ACAT IAM: DAE or as delegated ACAT IAC: Head of the DOD Component or, if delegated, the CAE

Table 5 cont'd. Description and Decision Authority for ACAT I–IV Programs. Source: USD(AT&L) (2013).

ACAT	Reason for ACAT Designation	Decision Authority
ACAT II	• Does not meet criteria for ACAT I or IA • Major system (10 U.S.C. 2302d) o Dollar value: estimated by the DOD Component head to require an eventual total expenditure for RDT&E of more than $185 million in FY 2014 constant dollars, or for procurement of more than $835 million in FY 2014 constant dollars o MDA designation (10 U.S.C. 2302)	CAE or the individual designated by the CAE
ACAT III	• Does not meet criteria for ACAT II or above • An AIS program that is not a MAIS program	Designated by the CAE
ACAT IV (Navy & Marine Corps Only)	• ACAT programs in the Navy and Marine Corps not otherwise designated as ACAT III are designated ACAT IV • There are two categories of ACAT IV programs: IVT (Test) and IVM (Monitor). ACAT IVT programs require Operational Test and Evaluation (OT&E) while ACAT IVM programs do not.	

2. General Services Agency

The General Services Agency (GSA) connects federal agencies to businesses to purchase or lease goods, services, and facilities through centralized procurement (General Services Agency [GSA], 2017a). GSA's (2017a) mission focuses on real estate, acquisition, and technology services where IT hardware products and services, or mobile devices, can be procured under "IT Schedule 70." IT Schedule 70 contains more than 7.5 million products offered by over 4,600 pre-vetted vendors that can be purchased through "eBuy," an online Request for Quotation (RFQ) tool and "GSA Advantage!," an online shopping tool used to purchase goods and services with pre-negotiated prices from pre-vetted vendors (GSA, 2017a). Under IT Schedule 70, DOD customers can purchase smartphones and tablets from manufacturers such as Samsung and LG. GSA also offers Assisted Acquisition Services (AAS), a comprehensive acquisition resource that provides customizable IT and professional services with scalable solutions that

combine technical, financial, acquisition and program management support for federal customers (GSA, 2017a).

3. Small Business Innovation Research/Small Business Technology Transfer

The Small Business Innovation Research (SBIR) program and Small Business Technology Transfer (STTR) program are federal programs aimed at small businesses to engage in R&D projects that foster innovation in support of federal agencies. Technology that has already been developed is not eligible for the SBIR/STTR programs. "SBIR [and STTR] funds the critical startup and development stages and it encourages the commercialization of the technology, product, or service, which, in turn, stimulates the U.S. economy" ("About Small Business Innovation Research [SBIR] | SBIR.gov," n.d., para. 10). The focus of SBIR/STTR is early stage R&D at small businesses, with topics of research designated by the participating federal agency. Small businesses are defined as "American-owned, organized as a for-profit entity, and have less than 500 employees" ("Tutorial 1: WHAT IS THE PURPOSE OF THE SBIR & STTR PROGRAMS? | SBIR.gov," n.d., para. 1).

According to the SBIR/STTR website, SBIR/STTR are organized in three phases. The first phase begins after the small business submits its proposal and is awarded by a federal agency "based on small business qualifications, degree of innovation, technical merit, and future market potential" ("Tutorial 1: WHAT IS THE PURPOSE OF THE SBIR & STTR PROGRAMS? | SBIR.gov," n.d., para. 5). Phase I (6–9 months) focuses on developing the concept of the idea or technology; Phase II (0–2 years) expands on Phase I work and is when R&D is conducted; Phase III is when the innovation is ready for private sector commercialization and is not funded by SBIR/STTR ("Tutorial 1: WHAT IS THE PURPOSE OF THE SBIR & STTR PROGRAMS? | SBIR.gov," n.d.).

SBIR eligibility is only for small business with 500 or fewer employees, for profit, and primarily U.S.-owned (51%) ("Tutorial 2: AM I ELIGIBLE TO PARTICIPATE IN THE SBIR/STTR PROGRAMS? | SBIR.gov," n.d.). According to the SBIR/STTR website, during Phase I, 67% of the research must be performed by the small

business, while up to 33% can be subcontracted out to either a non-profit or for-profit entity and during Phase II, the subcontracting limit goes up to 50%.

The main focus of STTR is the transfer of technology from a research institution (RI) ("Tutorial 2: AM I ELIGIBLE TO PARTICIPATE IN THE SBIR/STTR PROGRAMS? | SBIR.gov," n.d.). The SBIR/STTR website states, for STTR projects during Phases I and II, 40% of the research must be performed by the small business, 30% must be performed by a RI, and the remaining 30% is discretionary and can be outsourced to the RI or another subcontractor.

Although the SBIR/STTR programs use small, innovative companies to produce useful technology, this program is primarily for technology that still requires development. COTS solutions cannot be leveraged and the lengthy process of R&D for SBIR/STTR projects negate the benefits required for a timely solution.

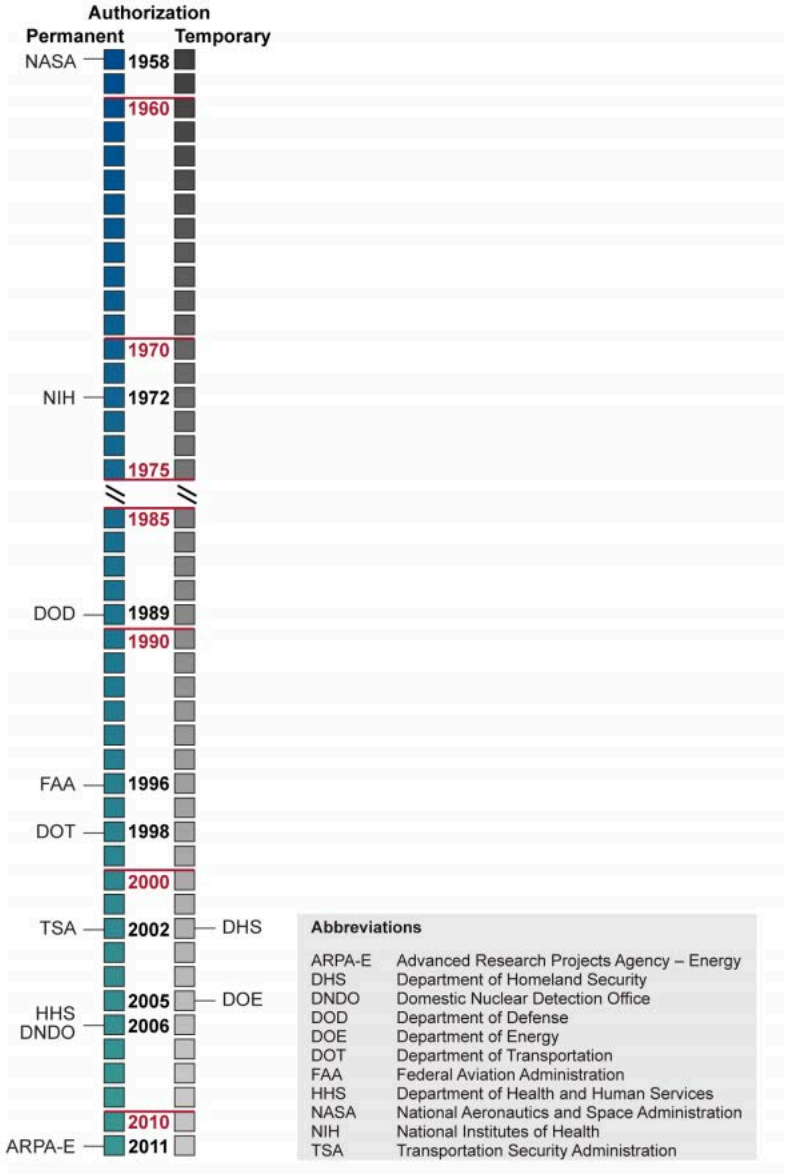
4. Other Transactions Authority

Other Transactions (OT) Authority is a special procurement vehicle better defined by what it is not: a contract, grant, or cooperative agreement (Halchin, 2011). Contracts are used to purchase goods and services and fall under the restrictions of the FAR; Grants are a financial assistance mechanism to "transfer a thing of value to the recipient to carry out a public purpose of support or stimulation"; Cooperative agreements are "written agreements between a federal laboratory and nonfederal partner to work together on a project" (Government Accountability Office [GAO], 2016, pp. 3-4). Congress created OT authority to allow certain agencies to develop agreements outside of the traditional methods of contract, grant, or cooperative agreement and not subject to the constraints of the FAR (Halchin, 2011). Elements excluded from OT agreements consist of "the Competition in Contracting Act, Truth in Negotiation Act, Contract Disputes Act, and the Procurement Protest System" (Egel, Guo, Lewis, & Webb, 2014, p. 19). The GAO report (2016), advantages of OT included the flexibility to customize transaction agreements to meet project requirements, attracting smaller non-traditional businesses, and speed in executing transaction agreements. Since OT functions outside of the FAR, it is also

difficult to quantifiably evaluate contractor performance, activities, and outcomes (Halchin, 2011).

Currently, 11 federal agencies (Figure 5) hold statutory authority to execute OT for one or a combination of research, development, and demonstration (RD&D), prototypes, or other activities (GAO, 2016). According to the GAO report (2016), most agencies expressed that flexibility to customize agreements with non-traditional entities was the primary reason for their use of OT. Non-traditional businesses who had not previous conducted business with the government had two concerns that was addressed through OTs: “protection of intellectual property and compliance with government cost accounting standards” (GAO, 2016, p. 12). Agencies typically acquired certain intellectual property rights from businesses, especially when the research was conducted using federal funds (GAO, 2016). OT allow the agreements to be customized to exclude the provisions for intellectual property found in traditional contracts (GAO, 2016). The GAO report (2016) found that non-traditional businesses “generally do not operate accounting systems in compliance with cost accounting standards, and that developing such systems can be cost-prohibitive” (p. 13) Using OT agreements allows non-traditional business to conduct business with the government without having to conform to government cost accounting standards (GAO, 2016).

Figure 5. Agencies with Permanent or Temporary Other Transaction Authority and Year Granted.
Source: GAO (2016).



Since OTs were introduced through the National Aeronautics and Space Act of 1958, temporary OT authority has been extended to 11 governmental agencies (Stevens, 2016). In an effort to streamline business transactions and reform defense acquisition, the 2016 National Defense Authorization Act (NDAA) established permanent OT authority (Stevens, 2016). Stevens (2016) describes four significant changes to OTs in the 2016 NDAA: 1) Non-traditional defense contractors are re-defined as not having entered a

traditional FAR-based contract at least one year prior to the date of OT; 2) To incentivize smaller, innovative businesses to participate, non-traditional defense contractors must be a significant participant of the OT agreement, otherwise traditional defense contractors must pay at least 1/3 of the cost; 3) Contracting Officer approval increased from $20M to $50M, SPE approval increased to $50M–$250M; and the Under Secretary of Defense (USD), Acquisition Technology and Logistics (AT&L) increased to anything greater than $250M; 4) Prototype agreements can lead to follow-on sole source production given the initial agreement was awarded based on the principle of competition and was completed successfully.

Although the DOD is authorized to execute OT for RD&D and prototypes, OT agreements were rarely used (GAO, 2016). The GAO report (2016) concluded that since OT agreements in the DOD were rarely used, OT agreements took longer to develop and execute than traditional contracting methods due to the lack of experience. Two DOD agencies that use OTs on a consistent basis are Defense Advanced Research Projects Agency (DARPA) and Defense Innovation Unit Experimental (DIUx).

5. Rapid Acquisition Units

Many rapid acquisition units throughout the DOD serve to address Urgent Operational Needs (UON). UONs are identified by the combatant commander to address issues that "seriously endanger personnel or pose a major threat to ongoing operations" (Chairman of the Joint Chiefs of Staff, 2005, p. GL-1). These rapid acquisition units include the Joint Rapid Acquisition Cell (JRAC), Rapid Equipping Force (REF), and Joint Improvised-threat Defeat Agency (JIDO). The JRAC was created by the Secretary of Defense to address immediate warfighter needs through flexibility of statutes, regulations, and color of money (Arellano, 2015). The REF was created by the Vice Chief of Staff of the Army (VCSA) to use robots to clear caves in Afghanistan during Operation Enduring Freedom (OEF) and broadened its mission to provide rapid solutions to address capability gaps for the Army (United States Army [USA], 2017c). The JIDO, formerly known as Joint IED Defeat Organization (JIEDDO), was created to search for solutions to combat improvised threats, such as IEDs, through preventative and counter-

defensive measures (DOD, 2017). Arellano (2015) demonstrated that the urgent needs procurement organizations had advantages that allowed them to be effective at rapid acquisition: the ability to recolor money without restrictions, waiving statuses and regulations, and the highest priority in support of combat operations in response to urgent needs statements (UNS). Urgent needs procurement organizations still exist, but the rate of UONs have decreased significantly in since 2015 (Arellano, 2015). Additionally, mobile devices are a materiel solution and without an urgent needs statement that leads to a mobile device solution, tools and methods used by rapid acquisition authorities to rapidly purchase mobile devices are not possible.

Other rapid acquisition units have emerged in recent years to expedite warfighter solutions for short-term needs through rapid prototyping and warfighter involvement. The Air Force's Rapid Capabilities Office (RCO) was activated by the Secretary of the Air Force in 2003 and its mission is to "expedite development and fielding of select DOD combat support and weapon systems" through current and emerging technology (United States Air Force [USAF], 2017, para. 2). According to the Air Force website, characteristics of the program include minimal chain of command, warfighter involvement, funding stability, and the issuance of waivers and deviations from directives and regulations as required. The Army RCO was modeled after the Air Force RCO and aims to "expedite critical capabilities to the field to meet Combatant Commanders' needs" through rapid prototyping and warfighter feedback "to address both urgent and emerging threats, while supporting acquisition reform efforts" (USA, 2017b, para. 1). The difference between the REF and Army RCO is the REF respond to UNS typically within six months and the RCO hits a an optimal time of one to five years to close capability gaps rather than provide immediate solutions or long-term development of a project (Lopez, 2016). Katrina McFarland, the Army acquisition executive stated "The goal of the Army Rapid Capabilities Office is not to procure systems to outfit the entire Army, but rather to use targeted investments to execute strategic prototyping, concept evaluation and limited equipping" (USA, 2017a, para. 10). The Navy created the Maritime Accelerated Capabilities Office (MACO) and the Marine Corps also created their own Marine Corps RCO based on the Air Force RCO, focusing on prototyping and

experimentation of mature technology first to fail quickly, identify issues, and learn before transitioning to a full program of record (Eckstein, 2016). The RCO and MACO are not new concepts; they are similar to the Advanced Concepts Technology Demonstration (ACTD) Joint Capabilities Technology Demonstration (JCTD). The ACTD/JCTD also emphasized early building and testing of prototypes before full-scale development to serve the COCOM (Aten, 2013). The completion of ACTD/JCTD result in multiple exit paths: termination, return to technology base for further development, residual utilization, initiate acquisition at Milestone B with major improvements, initiate acquisition at Milestone C with minor improvements, initiate acquisition at FOC as COTS or non-developmental items (NDI) (South, 2003).

Two constraints are preventing the defense services from fully executing the Rapid Capabilities Office model: funding and prototyping flexibility (Serbu, 2016). Funding flexibility is an issue because the DOD takes one year to prepare the budget, one year to justify the budget before Congress, and one year to execute the budget once funds are appropriated (Serbu, 2016). Lt. Gen. Michael Williamson, the Army's highest-ranking acquisition official, stated that the service chiefs need the freedom to be able to provide funding for prototyping and experimentation without tying them to major programs of record (Serbu, 2016).

6. Defense Advanced Research Agency

The mission of DARPA is to "create new, disruptive technologies in the interest of national security" (GAO, 2015a, p. 1). According to the Government Accountability Office (GAO) report, DARPA solicits proposals from thought leaders and innovators for general research to stimulate defense innovation. DARPA's unconventional structure and processes required funding flexibility outside of the traditional FAR and eventually received the authority to use OTs for major or rapid prototyping (Stevens, 2016). According to Stevens' (2016) interview with Scott Ulrey, DARPA primarily executes OTs for the SBIR program and for small businesses. Scott Ulrey stated that he had personally processed over 500 OT agreements and "DARPA has issued over 1000+ program solicitations with no legal issues" (Stevens, 2016, p. 32).

7. In-Q-Tel

In 1998, the Central Intelligence Agency (CIA) recognized a major information technology gap between the CIA and the private sector (Molzahn, 2003). To regain their competitive edge, the CIA needed to integrate itself within the innovation ecosystem and develop its relationships with the private sector (Molzahn, 2003). In-Q-Tel was created to model a "corporate strategic venture capital entity" by the CIA and make "equity investments in private-sector firms using government-supplied funds" (Reinert, 2013, p. 694). In-Q-Tel was structured as an independent entity from the CIA to maintain continuous rather than transactional relationships with industry to stay in tune with emerging technology (Reinert, 2013). The In-Q-Tel Interface Center (QIC) of the CIA communicates problem sets to In-Q-Tel, who in turn searches for private sector solutions tied to various startups (Reinert, 2013). By investing in the startup, In-Q-Tel secures an equity position in the company and a seat on its board of directors (Reinert, 2013). As an investor, In-Q-Tel is immediately aware of any advances or issues with the company or its technology (Reinert, 2013). Additionally, In-Q-Tel modeled DARPA's 'other transactions' method of procurement to induce flexibility and innovation in research & development (R&D) contracts (Yannuzzi, 2000).

8. Defense Innovation Unit Experimental

According to Carter (2016), DIUx was initiated by former Secretary of Defense Ash Carter to accelerate innovation in the DOD by bridging the gap between nontraditional industry partners and DOD. DIUx offices are centered within key technological hubs across the U.S., the first established in Mountain View, CA, also known as Silicon Valley, the second in Boston, MA, and the third in Austin, TX (Carter, 2016). According to Secretary Carter (2016), his intent for establishing DIUx was to develop "new partnerships with the private-sector and technology communities" (para. 12). Relationships with and proximity to key technology partners allow access to emerging innovations that can be leveraged within the DOD.

DIUx introduced a first-of-its-kind acquisition instrument called the Commercial Solutions Opening (CSO) to "leverage the extensive amount of commercial R&D

investment and quickly access cutting-edge technology" (Defense Innovation Unit Experimental [DIUx], 2016, p. 2). The CSO allows non-traditional companies to overcome the high barriers to entry and long lead times of the federal acquisition system through OT for prototype projects (DIUx, 2016). OT is not a new process, but since it is not regulated under the FAR, they "are not required to comply with the FAR, its supplements, or laws that are limited in applicability to procurement contracts" (USD(AT&L), 2002, p. 8). The DOD's intent was to attract nontraditional defense contractors, defined as a business unit who has not entered into or performed on any FAR-based contract one year prior to the OT agreement (USD(AT&L), 2002).

DIUx (2016) stated that the CSO process begins with a posting of area of interest (AOI) from a DOD customer on its website. "AOIs describe problems to be solved or particular technologies we are interested in, not detailed specifications and requirements" (DIUx, 2016, p. 10). Vendors then submit a short solution brief that only describe the company's technology and the company itself. According to DIUx (2016), DIUx uses a three-phased approach to evaluate the submissions. Phase I, Evaluation, evaluates vendors based on four criteria: relevance, technical merit, business viability, and innovation. Phase II, Pitch, allows the opportunity for vendors to pitch their solution to DIUx leadership. Additional evaluation criteria in Phase II include: cost, schedule, and data rights. Upon evaluation, the DOD customer will select one or more prototype options and a Request for Prototype Proposal (RPP) will be issued to the vendor. The vendor is required to develop the Statement of Work (SOW) in collaboration with DIUx and the DOD customer. Phase III, Proposal, evaluates the final proposal from the vendor and DIUx negotiates and awards the OT (DIUx, 2016).

DIUx's CSO process offers a few advantages. Firstly, vendors have minimal barriers to entry: There are no requirements to register in a database system of vendors and a short solution brief to an AOI posting does not require huge time or resource commitments that comes with bidding on a contract. Second, due to its locations residing in major innovation hubs around the nation, DIUx has greater access to a broader range of innovation solutions through its networks. Third, speed: prototype contracts can be awarded within a few months.

D. CURRENT CAPABILITIES AND EQUIPMENT

There is no doubt that mobile devices have been used in the DOD for some time, and are continuing to be researched and explored for new uses. As early as March 2005, BlackBerry support and use for the DOD faced the real threat of being eliminated while undergoing legal issues with patent infringement. A year later, the DOD released a brief citing that "the BlackBerry was crucial for national security given the large number of government users" (Bouchoux, 2016). Recently, mobile devices, specifically commercial smartphones, have increasingly become the centerpiece and focus of effort of several research and development programs (Kaul, Makaya, Das, Shur, & Samtani, 2011).

Current smartphone platforms integrate hardware and software in one device to provide unparalleled capabilities including GPS, accelerometers, cameras (both still and video) and several different methods of wireless and wired connectivity (Oregon, 2011). Current fielded mobile device capabilities within the DOD include, but are not limited to: Kinetic Integrated Low-Cost Software Integrated Tactical Common Handheld (KILSWITCH)/Persistent Close Air Support (PCAS), Marine Air Ground Task Force (MAGTF) Common Handheld, NETT Warrior, CSfC (NSA), and BlackBerry (AT&T).

1. KILSWITCH/PCAS

KILSWITCH and PCAS are both examples of tactical applications developed for use on mobile devices. Both systems seek to enable the use of mobile devices as extensions of a JTAC (Joint Terminal Attack Controller), and to increase the lethality and capability of both CAS and ground fires in a tactical environment.

PCAS started in 2010 by DARPA to increase the effectiveness and lethality of CAS. The ground segment of PCAS would enable JTACS to call in CAS while increasing their mobility, situational awareness and communication ability (Defense Advanced Research Projects Agency [DARPA], 2016). The system was envisioned to be used on Android based tablets, and the application could be downloaded with current information. From December 2012 to March 2013, DARPA fielded 500 Android-based tables to units in Afghanistan, which allowed the PCAS-enabled units to coordinate CAS engagements much more effectively (DARPA, 2016). The first complete and full scale

integration of PCAS occurred in March 2015 during TALON REACH, hosted by the Marine Corps.

PCAS led to the Marine Corps specific development of KILSWITCH, which is the Marine's version of PCAS. Developed in coordination with DARPA, it is essentially the same application with slight modifications. KILSWITCH is able to be used on an Android tablet, and connect via COTS Wi-Fi or wired solutions to a radio, such as a AN/PRC-117G, to communicate and connect to the tactical backbone and C2 hub (Staten, 2015). Both these applications display the emerging capabilities that mobile devices will play in the tactical battlefield of the future.

2. MAGTF Common Handheld

MAGTF Common Handheld seeks to obtain one commercial device that will satisfy all the military necessary requirements while being able to be used in a tactical environment (Rockwell, 2016). As early as 2009, the Marine Corps Warfighting Laboratory (MCWL) recognized the need to incorporate handheld devices into their Reconnaissance, Surveillance and Target Acquisition (RSTA)overall scheme (Marine Corps Warfighting Laboratory [MCWL], 2009), and Marine Corps Systems Command (MARCORSYSCOM) has recently expanded this into the MAGTF Common Handheld program under MARCORSYSCOM C3.

Current civilian versions of similar type systems exist and are currently fielded by some law enforcement agencies and emergency responders. One such system is Motorola's Premier One, Smart Public Safety Solutions which seeks to link first responders (fire, EMS, police) with dispatchers and callers to reduce the time necessary for first responders to reach the response location (Motorola, 2016). The system even supports text messages, GPS locations and pictures sent by 911 callers that can be routed, screened and sent by dispatchers to first responders.

MAGTF Common Handheld seeks to do many of the same things as Motorola's Smart Public Safety Solutions (SPSS) on a squad and platoon level, including streaming of web-based video, voice and data that may include targeting, position, location and

identity (PLI) and logistical information (Sotire, 2010). While relatively new, devices are scheduled to be fielded to squad leaders as early as 2019 (Browne, 2016).

3. NETT Warrior

NETT Warrior was the evolution of the Army's original Land Warrior system (later named the Ground Soldier System), just one of many small programs in the Army's overall Future Combat System. Envisioned as an "integrated dismounted Soldier system…that provides un-paralleled SA [situational awareness], allowing faster and more accurate decisions in the tactical fight" (Copeland, 2011).

NETT Warrior uses a mobile handheld device connected to a radio, similar to KILSWITCH and PCAS to perform its intended mission. In 2013, Program Executive Office (PEO) Soldier chose the Samsung Galaxy Note II as its preferred handheld device for use with the system (Dixon and Henning, 2013). Jason Regnier, a project manager with the NETT Warrior project also stated "the ability to buy new devices means having the latest technology and processors available" (Dixon et al., 2013).

Initial Operational Testing and Evaluation (IOT&E) conducted in 2015 did reveal several flaws with the system as a whole, but none of these were directly attributed to the End-User Device (Samsung Galaxy Note 2) (DOT&E, 2015). The report even goes so far as to say that the intent is for the device to be changed or updated every 18 to 24 months as the commercial market produces devices that are increasingly more capable. It is clear that the Army has planned for device obsolescence and failure during its initial plan for NETT Warrior, and intends to continually purchase new devices as they are available on the commercial market.

4. Commercial Solutions for Classified Program

The CSfC program seeks to obtain certification for mobile devices from the NSA for use on various types of classified applications, including both hardware and software. The NSA has realized that U.S. Government customers (to include the DOD) are increasingly requiring the latest and most modern version of commercial devices to meet mission objectives (National Security Agency [NSA], 2016). One of the prime

advantages of the CSfC program is device National Information Assurance Partnership (NIAP) evaluations in as little as 90 days, which previously took up to 180 days to complete (NSA, 2016). The NIAP provides a third party certification of CSfC solutions based on the Common Criteria Process, ensuring that all CSfC solutions meet the required security requirements that are deemed acceptable by the NSA. Previously, the government has relied on devices that have been designed by the government and certified during development for use on classified systems (Scott & Spanel, 2016).

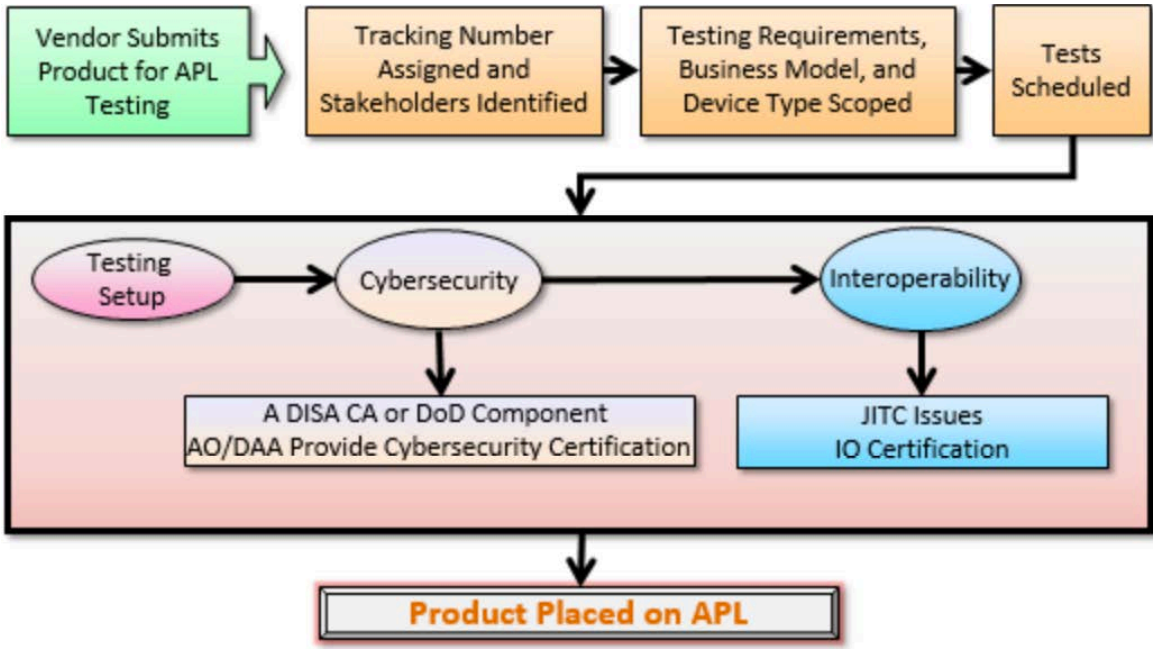
Many of these GOTS systems, as with previous government acquisition projects, were capability specific and only filled the need of one requirement, often resulting in duplicate systems for small changes in requirements. The NSA CSfC provides much more rapid capabilities adoption and certification to the DOD, allowing the DOD to leverage newer and more modern hardware and software (to include mobile devices), while increasing flexibility and lowering future costs. CSfC allows the DOD to leverage the COTS solutions (specifically hardware) faster development and release schedule when compared to GOTS developed solutions. Some of the mobile devices on the NSA CSfC components list at the time of this writing include: BlackBerry 10.3 OS, Apple iOS 9, Microsoft Surface Book (Windows 10) and Samsung Galaxy S4, 5, 6 and 7. The CSfC components list offer additional capabilities, such as MDM and IPSec virtual private network (VPN) Clients.

5. DOD Information Network Approved Products List

According to DOD CIO (2014b), IT must be certified for interoperability to meet the Net Ready KPP within the DOD Information Network (DoDIN). The DISA JITC was directed to “evaluate and certify joint, multinational, and interagency IT interoperability for the DOD (DOD CIO, 2014b, p. 11). As is demonstrated in Figure 6, the DoDIN Approved Products List (APL) process provides Interoperability certification by JITC and cybersecurity certification by DISA or DOD component certifying authority (CA) (Defense Information Systems Agency [DISA], 2017). All devices on the DoDIN APL are DISA certified to operate on unclassified DOD networks. Once certified, devices remain on the DoDIN APL for a period of 3 years before their certification expires.

Devices may have their certification revoked earlier, however this generally happens when a new software version (i.e., iOS 10 vs. iOS 9) is evaluated on the same device. This simply requires that the device be upgraded with new software and it will be approved on the DoDIN APL.

Figure 6. Standard Process for DoDIN APL Certification



6. BlackBerry

BlackBerry has long been the preferred government and DOD COTS solution for mobile communication. BlackBerry was the first mobile device management (MDM) provider to receive a full Authority to Operate (ATO) by DISA in Aug. 2013 (Cheng, 2014). BlackBerry was also the first company to have a device certified on DISA's Approved Product List in August of 2015 (DISA, 2016). This was quickly followed (within several weeks) by many other approved devices including, Samsung, LG, and Microsoft, but still represents a significant accomplishment for BlackBerry. This means that current BlackBerrys operating the approved OS and on approved devices are certified according to DoDI 8100.04 and meet current Information Assurance/Cyber Security and Interoperability standards.

In addition to the DOD, BlackBerry has been at the forefront of international and U.S. government approval for its devices. This includes the United Kingdom, NATO, U.S. Senate and U.S. Coast Guard (Greene, 2016). BlackBerry currently remains at the forefront of DOD and government usage, however DOD's CMD Implementation Plan is calling for 600,000 mobile devices with focus on a device-agnostic approach that can be tailored by the user (Anderson and Rutherford, 2013).

E. CHALLENGES OF MOBILE DEVICES

The characteristics of mobile devices pose unique challenges from desktop and laptop computers due to their "size, portability, always-on wireless connection, physical sensors, and location services" (CIO Council, 2013b, p. 4). The security objectives of confidentiality, integrity, and availability frame the challenges of device security, mobile computing architecture, and network infrastructure for mobile devices (Souppaya & Scarfone, 2013). Additionally, mobile devices must meet rigorous federal and DOD IT standards and once the standards are met, also face numerous challenges within the DAS.

1. Device Security

The ease of carrying mobile devices due to their size and portability increases the likelihood of the devices becoming lost or stolen and compromising its data (Souppaya & Scarfone, 2013). The decision to store data on the device or virtualize it using a client based approach must be made to mitigate attacks or prevent recovery of data from unauthorized users (Souppaya & Scarfone, 2013). Secure encryption methods to protect the data, especially when implemented within a layered defense, increase the length of current validation processes (CIO Council, 2012b). The CIO Council (2012b) concluded that Personal Identity Verification (PIV) on mobile devices may pose a problem due to the difficulty to carry out two-factor authentication methods. Additionally, strong authentication needs to be careful not to sacrifice the warfighter's ease of use when handling mobile devices (CIO Council, 2012b).

2. Mobile Architecture

Mobile architecture includes four key areas: mobile device management (MDM), mobile application management (MAM), identity and access management (IAM), and data management (CIO Council, 2013b). Centralized MDM must be implemented to ensure all devices are configured uniformly and securely, usage and functional limitations are in place, and updates occur in a timely manner (CIO Council, 2013b). In the event a mobile device is lost or stolen, MDM can initiate a remote lock or wipe its data (CIO Council, 2013b). MAM controls the secure development of applications, guards against malicious applications, and manages the application life-cycle through remote upgrades or uninstalls (CIO Council, 2013b). IAM offers a variety of solutions to enforce PIV to access sensitive data through Bluetooth protocols, PIV card reader "sleeves" for devices, and NFC (CIO Council, 2013b). Data management covers both data governance or categorization to allow the sharing of information and data encryption to allow the sharing of data across unsecured networks (CIO Council, 2013b).

3. Network Infrastructure

Mobile devices are designed to operate across wireless infrastructures, such as cellular, Wi-Fi, and Bluetooth. The challenge is that the connection can range from "trusted (secure enterprise wireless network), untrusted (public Wi-Fi), or hostile (foreign telecom provider's network)" (CIO Council, 2013b, p. 2). Utilization of a VPN to connect to DOD networks will be a critical means to securely transmit and receive sensitive information in such environments.

4. DOD IT Standards

IT and National Security Systems (NSS) interoperability and supportability across the DOD enables availability of information and cybersecurity to support net-centric operations using the current GIG, and the future JIE (DOD CIO, 2007). The DOD CIO (2007) defined GIG as:

> The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing,

> disseminating, and managing information on demand to warfighters, policy makers, and support personnel. (p. 13)

IT standards in the DOD are identified, developed, and prescribed "to promote interoperability, information sharing, reuse, portability, and cybersecurity [replacing information assurance (IA)]" and can be found in the DOD IT Standards Registry (DISR) (DOD CIO, 2015, p. 2).

Cybersecurity is regulated under DOD Instruction 8500.01 (2014) for IT products. The extensive list cybersecurity requirements include: unified capability certification, classified product guidance from the Committee on National Security Systems (CNSS) and the NIAP, security configuration guidance, connection approval, protection of mission critical functions, integration of cybersecurity in the DAS, developmental and operational test, risk assessment, enterprise architecture principles and guidelines, Defense Information System Network (DISN) connection approval procedures and processes, National Institute of Standards and Technology's (NIST) Security Content Automation Protocol (SCAP) standards, and Controlled Unclassified Information (CUI) and operations security (OPSEC) standards.

5. Defense Acquisition System Challenges

Although the RAND study conducted by Porche et al. (2012) addressed improving the IT acquisition process for computer network defense (CND) programs of record, the analysis and recommendations are also applicable to mobile devices. The U.S. Navy's Program Executive Office for Command, Control, Communications, Computers, and Intelligence (PEO C4I) identified the following challenges for IT programs within the DAS: 1) Timeliness of requirement approval, 2) Excessive documentation requirements, 3) Time-consuming contracting process, 4) Unstable funding and program objective memorandum planning, and 5) Lengthy testing, certification and accreditation (C&A), and installation processes (Porche et al., 2012). Porche et al. (2012) provided additional follow-on challenges to include "configuration management, change control, and the need for constant patching" (p. xiii).

F. ACQUISITION SCHEDULE PERFORMANCE

The traditional defense acquisition cycle is being outpaced by technology advancements, resulting in its obsolescence by the time the product gets into the hands of the warfighter (Tate, 2016). Cycle time is defined as from formal program initiation or funding approval at Milestone B to initial operational capability (IOC) (Tate, 2016). According to Takai (2012), major automated information systems (MAIS) had an average cycle time of 91 months, which was two to three times the industry average for IT refresh cycle time. Riposo, McKernan, and Duran (2014) proposed that schedule improvements may come in many forms such as tailored reporting and oversight, waivers, or the use of commercial technology. "Improving a schedule is about meeting the mission and threat in a more timely fashion" (Riposo et al., 2014, p. xii).

In analyzing the acquisition documents from the 1960s to present, (Riposo et al., 2014) found that the most common reasons for schedule delays were: the mismanagement of technical risk, "initial assumptions or expectations that are difficult to fulfill," and funding instability (p. x). Table 6 provides a more detailed list of possible reasons that contributed to schedule delays.

Table 6. Reasons for Prolonged Schedules and Schedule Slippage. Source: Riposo et al. (2014).

Area	Possible Reason
Requirements development, generation, and management	Infeasible or unrealistic requirements
	Unstable requirements (e.g., engineering requirements, readiness requirements, reliability and support requirements)
	Inefficiencies in the process (e.g., serial nature of process and requirements evolution)
Managing technical risk	Excessive technical, manufacturing, or integration risk (general) or program complexity
	Unanticipated design, engineering, manufacturing, technical difficulty, or technology integration issues
	Overly optimistic assumptions/expectations (technical risks, performance goals, system requirements, or design maturity)
	Immature technology
	Concurrency in complicated programs
	Prototyping
	Deficient test planning or testing inefficiencies
	Inadequate funds for testing
Resource allocation	Funding instability or budget cuts
Defense acquisition management	Lack of focus on schedule or inadequate schedule management (e.g., underutilization of integrated master schedule)
	Overly optimistic assumptions/expectations in general, including insufficient contingency funds in program budgets
	Overly optimistic assumptions/expectations in cost and schedule estimates
	Personnel issues
	Competition
	Use of undefinitized contract actions
	Contractor performance and inadequate incentives
	Inadequate tailoring of the acquisition process
Other	Delays in obtaining necessary data

Riposo et al. (2014) concluded that the primary method for reducing schedule delays and growth was developing "strategies that manage or reduce technical risk" (p. xii). Based on previous literature, Riposo et al. (2014) compiled a list of possible ways to improve schedules (Table 7).

Table 7. Possible Ways to Improve Schedules.
Source: Riposo et al. (2014).

Area	Possible Ways to Improve Schedules
Requirements development, generation, and management	Stable and realistic initial requirements, especially at the engineering level
	Better collaboration between the program management and end-user communities (with proper management)
	Proper management of flexible requirements
Managing technical risk in development and production	Use of mature/demonstrated technology to ensure a high level of maturity before production
	Use of incremental fielding or EA strategies and the development of derivative products (rather than brand-new designs)
	Employment of "agile" methods that can easily adapt to changes in software development
	Prototyping
	Concurrency in programs with low technical risk
	Use of commercially derived items
	Use of the commercial practice of freezing the design before the production contract award
	Use of the commercial practice of reducing the design's complexity
Resource allocation	Stable funding
	Adequate test funds (hardware, modeling and simulation)
Acquisition management: internal to the program	Bypassing competition during production (including employing multiyear or sole-source procurement strategies in the production phase)
	Preplanned product improvement
	Acquisition of the same number of units but in larger, more economical quantities in the production phase
	Emphasis and adherence to schedule as a program priority
	Development and maintenance of a comprehensive and realistic master schedule

Table 7 cont'd. Possible Ways to Improve Schedules. Source: Riposo et al. (2014).

Area	Possible Ways to Improve Schedules
Acquisition management: internal to the program (continued)	Use of contracting vehicles to expedite contracting process (e.g., existing contracts, undefinitized contracts in low-rate initial production, sole-source contracts)
	Operational testing and evaluation results available before production startup
	Use of modeling and simulation to reduce the risk and duration of live tests
	Involvement of the test community in all program phases
	Use of integrated product teams
	Improved program stability in general, including funding and requirements
	Realistic schedule estimates
Acquisition management: external to the program	Senior leadership support
	Program identified as a priority

The shift to COTS can be contributed to its reduced acquisition cycle time primarily from decreased design and engineering time and also from decreased testing requirements (Gutierrez, 2002). Although commercial items may provide cost savings, this is not always the case. Component and integration testing cannot be avoided because commercial items are not tested for a military environment (Gutierrez, 2002). A gap will exist between the DOD and commercial use and modifying a commercial item to bridge that gap may result in technical problems and cost overruns (OSD, 2000). Two ways to manage the risk of commercial items are early involvement of the Service's Operational Test Agency for testing requirements and early testing in operational environments (Gutierrez, 2002). To reduce the acquisition cycle, Porche et al. (2012) recommended that programs "pursue approval authorities at the lowest appropriate level" (p. 34). An example would be to designate the PM as the MDA or the PEO as the decision accreditation authority to reduce approval times (Porche et al., 2012).

III. DATA

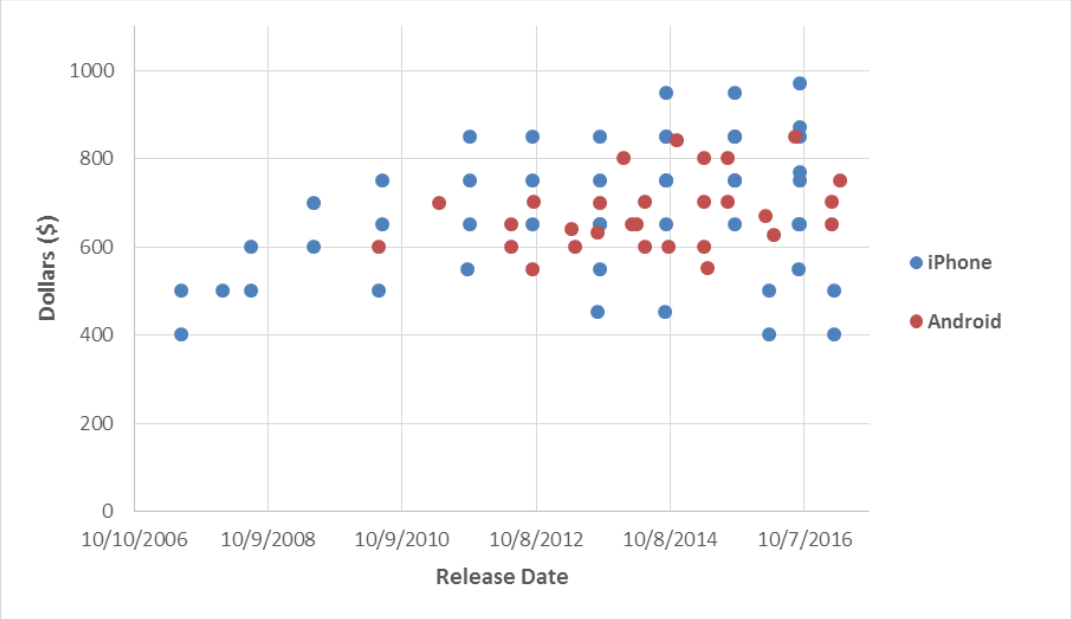
A. COMMERCIAL CELL PHONE DATA (IPHONE AND ANDROID)

Commercial cell phone data regarding cost, phone performance/hardware characteristics, release dates and production end dates was obtained from various sources. Phones that had readily available data included the iPhone (iPhone Original through iPhone 7 Plus), LG G Series (Optimus G Pro through LG G6), Samsung Galaxy S Series (S2 through S8) and the Samsung Galaxy Note Series (Note 2 through Note 7). A total of 75 data points were evaluated from 39 different commercially available phones. Several individual models had multiple variants, stemming exclusively from differing onboard memory options (i.e., iPhone 6S with 16, 32, 64, and 128GB options).

1. Cost

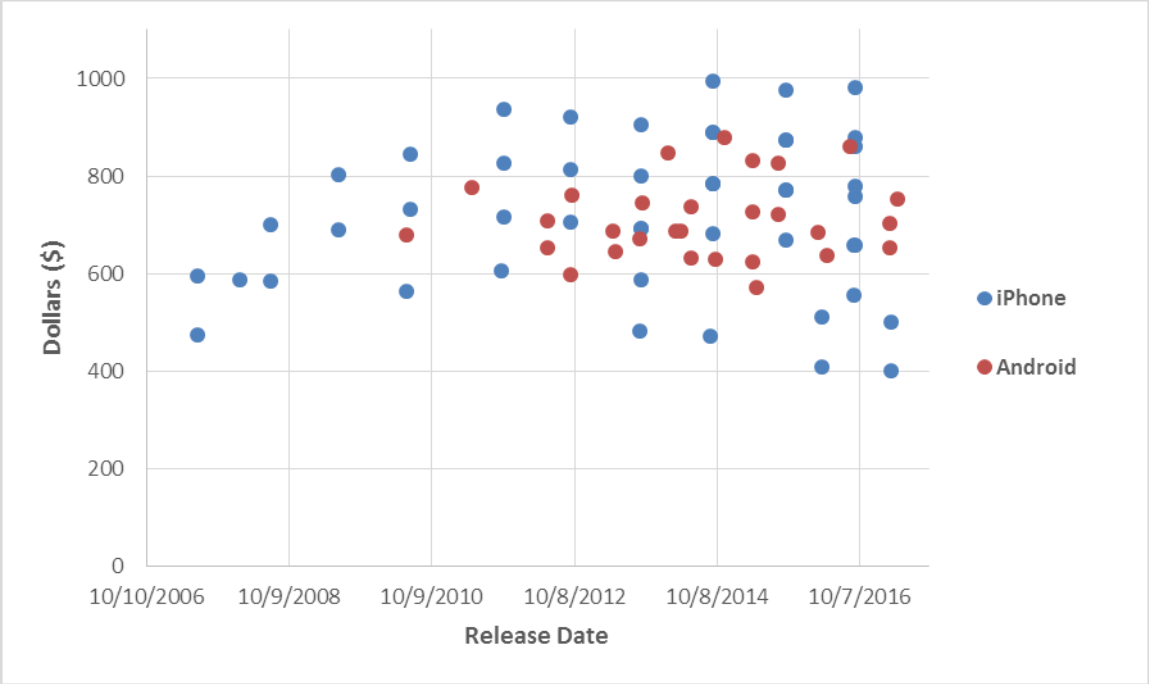
The cost at release of a phone was taken using the lowest, commercially available non-contract price from a reputable vendor (TMobile, Verizon, AT&T, etc.) at the release date, as shown in Figure 7.

Figure 7. Cost of Phone at Release Date



Using an inflation rate of 1.76%, taken from the average CPI increase from 2007 to 2016 (10 years) (Bureau of Labor Statistics, 2017), the cost of the phones in 2017 dollars was calculated (Figure 8).

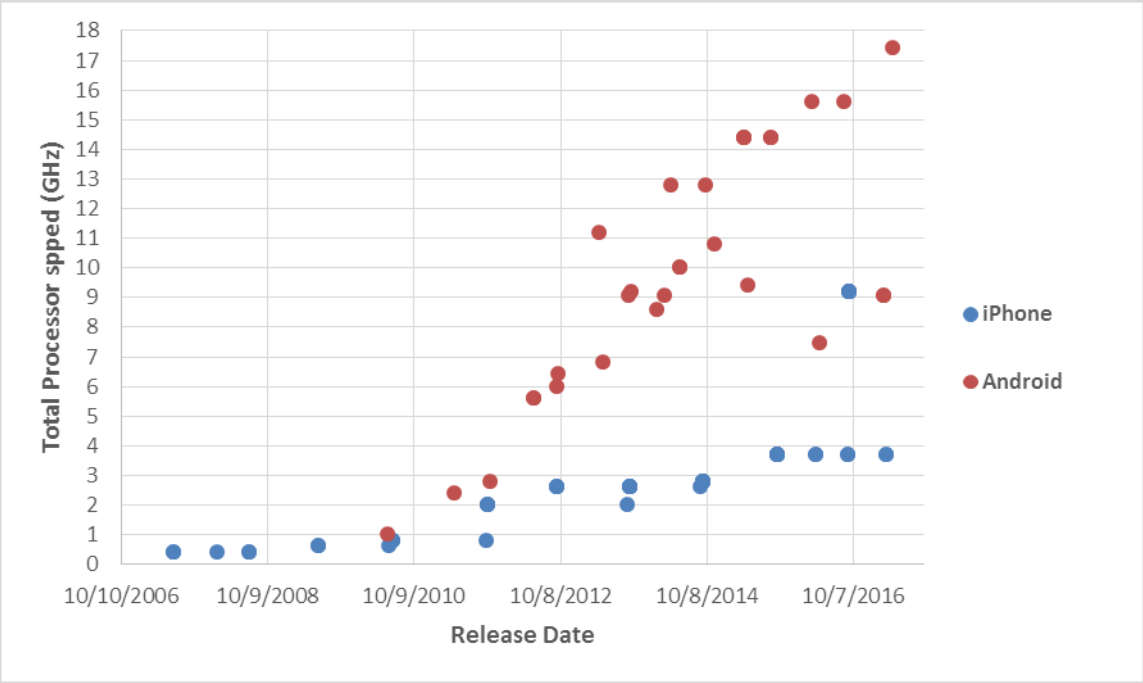
Figure 8. Cost of Phone in 2017 Dollars



2. Processor Speed

Total processor speed (Figure 9) was calculated by totaling all of the clock rates for each processor (for those phones with Dual-Cores, Quad-Cores, etc.) and adding them together to obtain an aggregate total for each phone. Several phones have multiple cores, but often only a few of the cores are the highest speed, which is the speed that is advertised. The other cores have lower clock rates (e.g. Samsung Galaxy S7 has 4x 2.3 GHz and 4x 1.6 GHz cores).

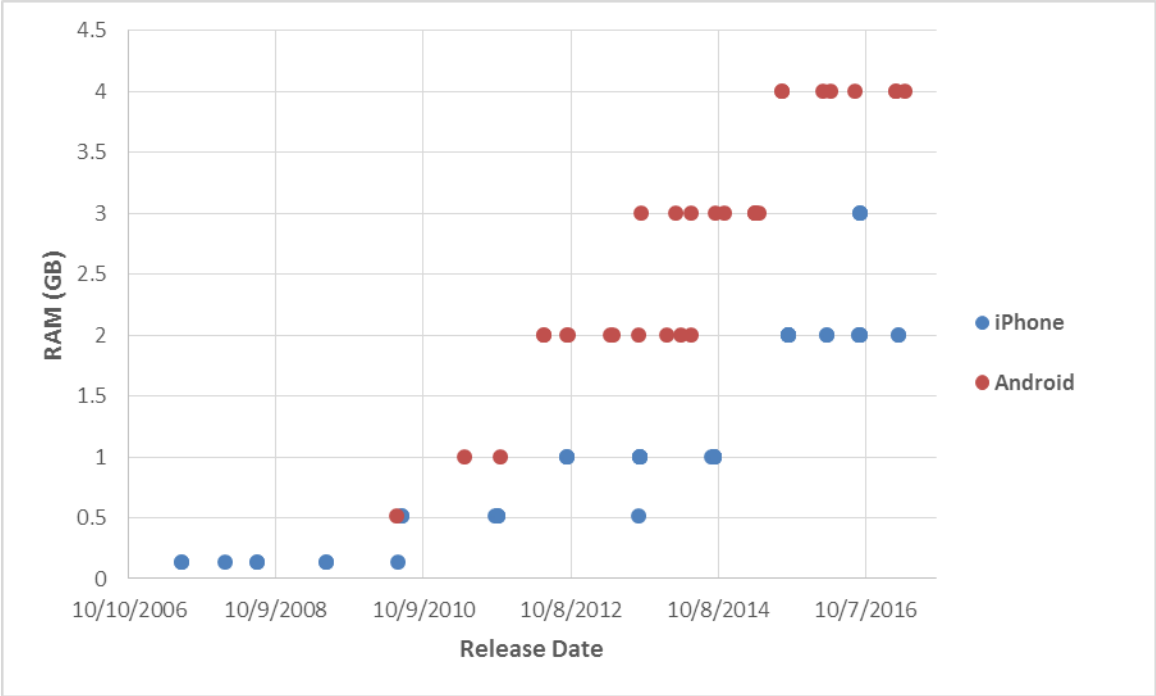
Figure 9. Total Processor Speed for Phones



3. RAM

The total amount of RAM (Figure 10) per phone was evaluated. Horizontal lines indicate that several different models and types of phones have the same RAM, and follow the typical numerical increasing trend of 512MB, 1GB, 2GB, etc., seen in modern computers.

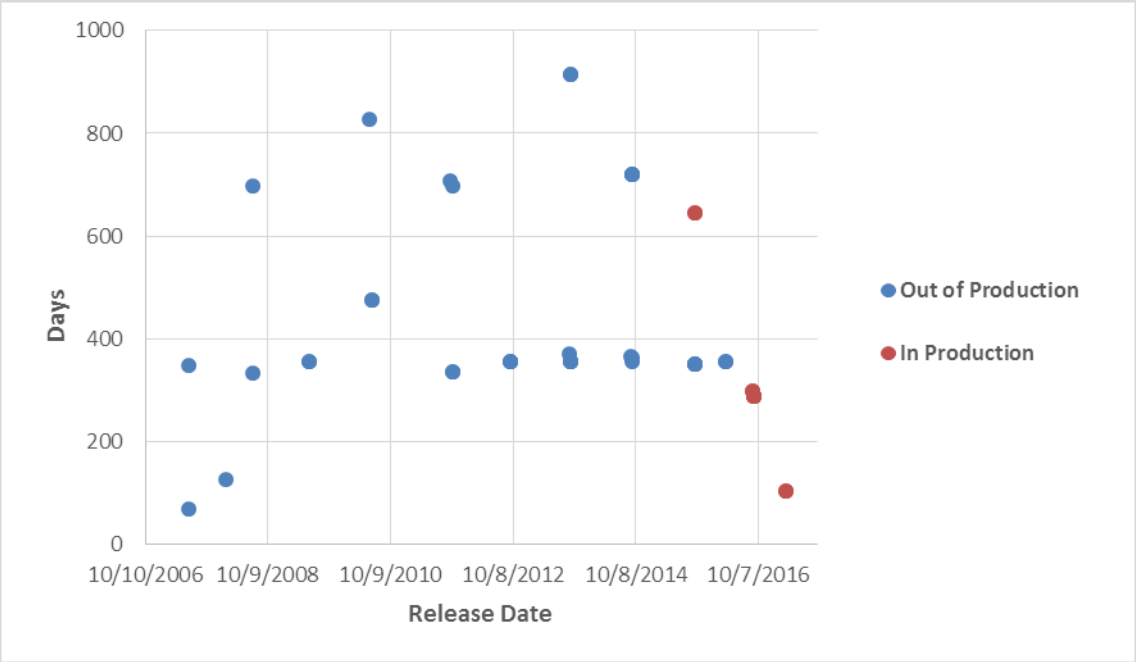
Figure 10. RAM



4. Life Cycle

Official production end dates were only available for iPhones, since many Android phones can be discontinued in one country or region but continue to be produced for sales in other areas. This resulted in confusing and conflicting information for official end dates of productions of most Android phones, so that data was not included. The iPhone data provided 48 data points across 15 different phones. To calculate a phones total life cycle in days, the difference between its official release date and official end production date was taken. This gave a length in days that the individual model phone was produced and available for purchase from the manufacturer (barring any excess inventory after the production end date) (Figure 11).

Figure 11. Life Cycle of iPhones



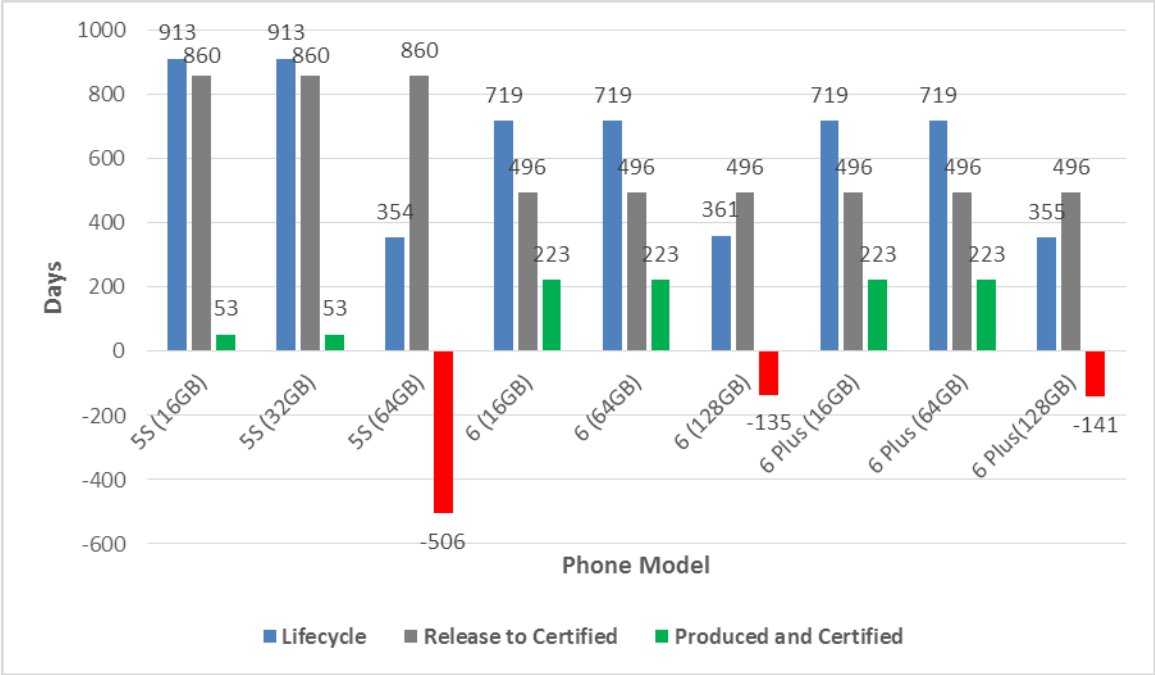
B. CSFC APPROVAL/CERTIFICATION

Once a product is certified, it is posted on the NSA's CSfC Components List along with the NIAP Validation Report. The date of publication of the NIAP Validation Report is the date that the device can officially be used as an approved CSfC device. Validations are done on specific hardware and software configurations (i.e., iOS 9.2 with iPhone 6 Plus). Individual validations may cover several different hardware and software configurations that are similar in nature.

1. iPhone Data

By comparing the certification date of the NIAP Validation Report against the official end production date, the time individual iPhone models were in production and CSfC certified could be calculated. As shown in Figure 12, the amount of time an individual iPhone model was in production until it was certified, which was also obtained by comparing the certification date against the official release date.

Figure 12. iPhone CSfC Data

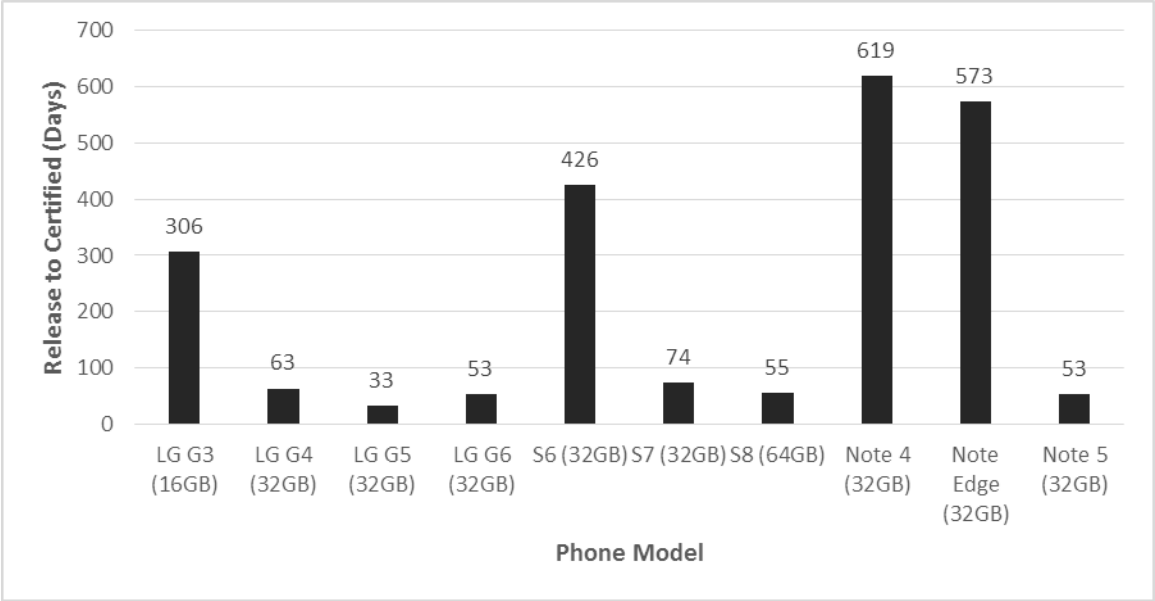


A Produced and Certified column in red (corresponding to negative days) indicates that particular individual phone model was certified by CSfC after the official end production date. Of note, there are no currently produced iPhones that are CSfC certified. NIAP started validating iOS 10.2 on an unspecified number of iPhones and iPads on March 10, 2017 with an unknown completion date (National Information Assurance Partnership [NIAP], 2017).

2. Android Data

As previously mentioned, Android official end production dates were confusing and difficult to come by. Only the amount of time from official release to CSfC certification of differing Android models (LG G Series, Samsung Note Series, Samsung S Series) was evaluated and shown in Figure 13.

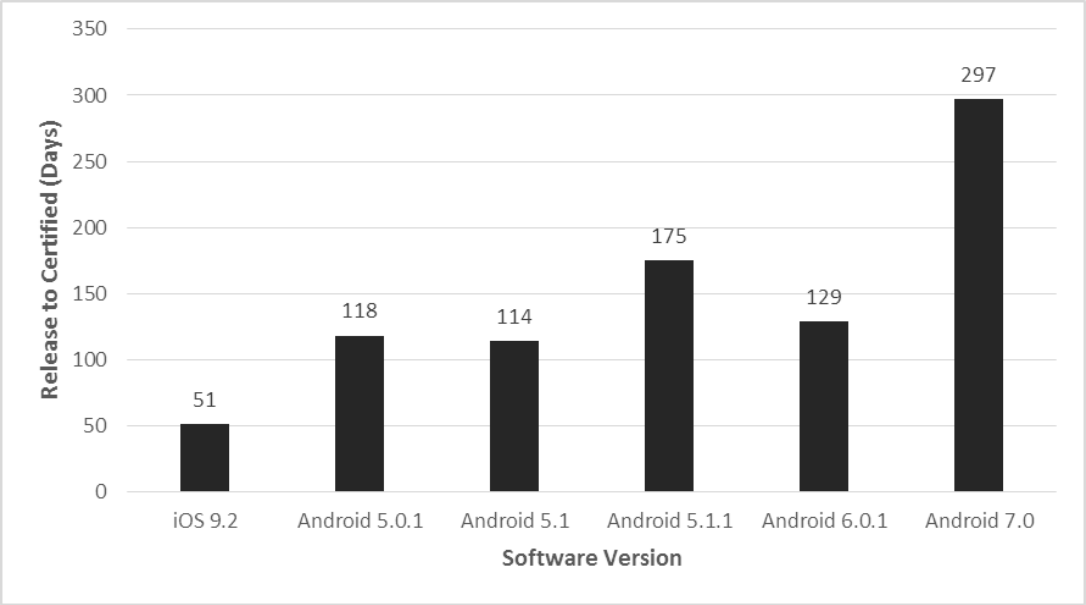
Figure 13. Android Phones CSfC Certification Time



3. Software Data

Similar to the Android data, the software version of the different phone models at certification time was evaluated against the release date of that software version to determine the amount of time between a software release and CSfC certification as displayed in Figure 14. There often exists a significant delay between when a software update is first release by the manufacturer and then receives CSfC certification with a trend that the delay appears to be getting longer.

Figure 14. Software CSfC Certification Time



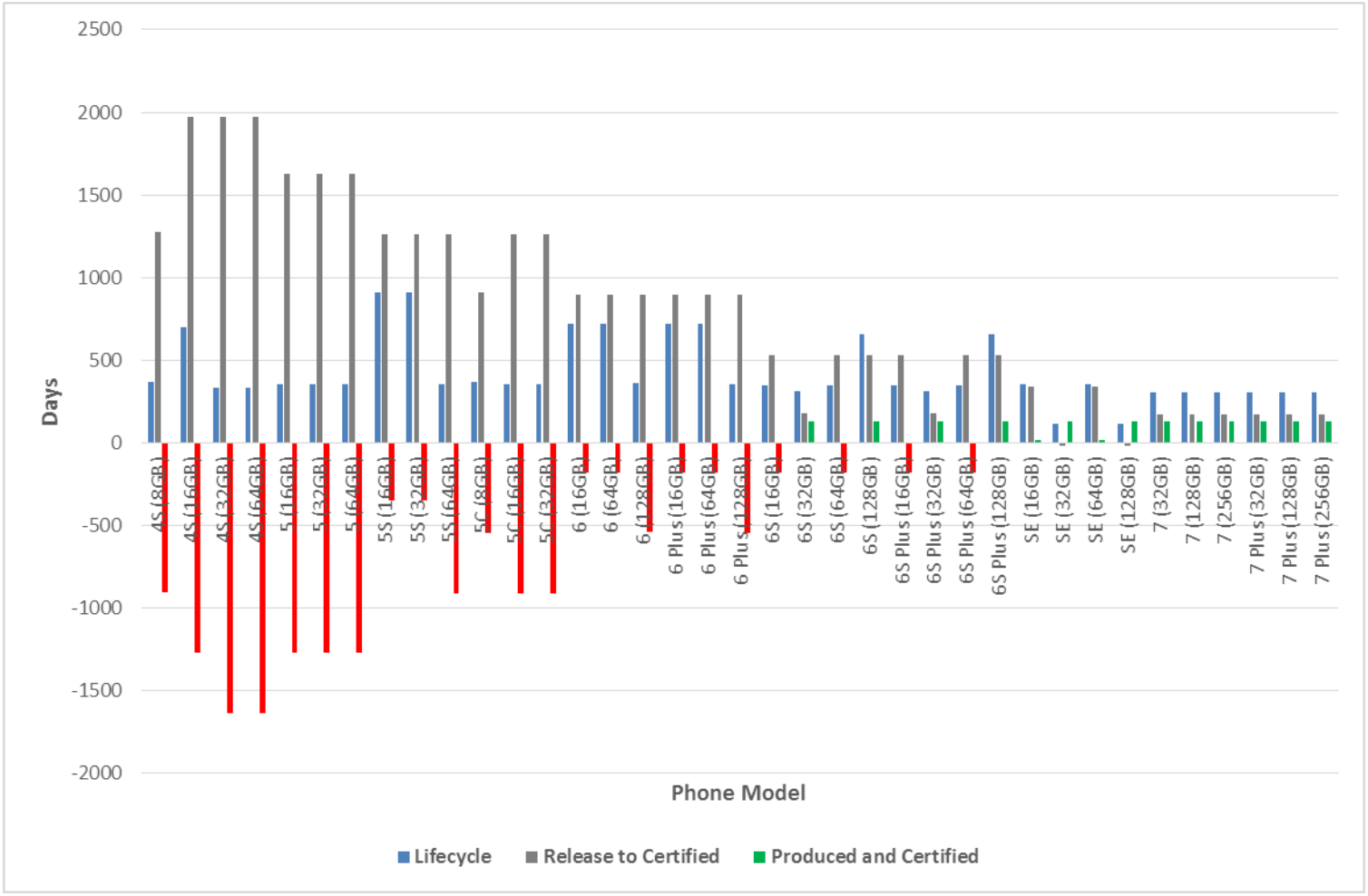
C. DODIN APL APPROVAL/CERTIFICATION

The same methodology for NSA CSfC certification timelines was applied to the DoDIN APL.

1. iPhone Data

The amount of time needed for iPhones to become certified on the DoDIN APL is displayed in Figure 15. The red lines in Figure 15 indicate that the individual model phones had their production halted before they were certified, while the green lines indicate the amount of time the phones were produced for after DoDIN APL certification (with many still currently in production at the time of this writing).

Figure 15. iPhone DoDIN APL Data

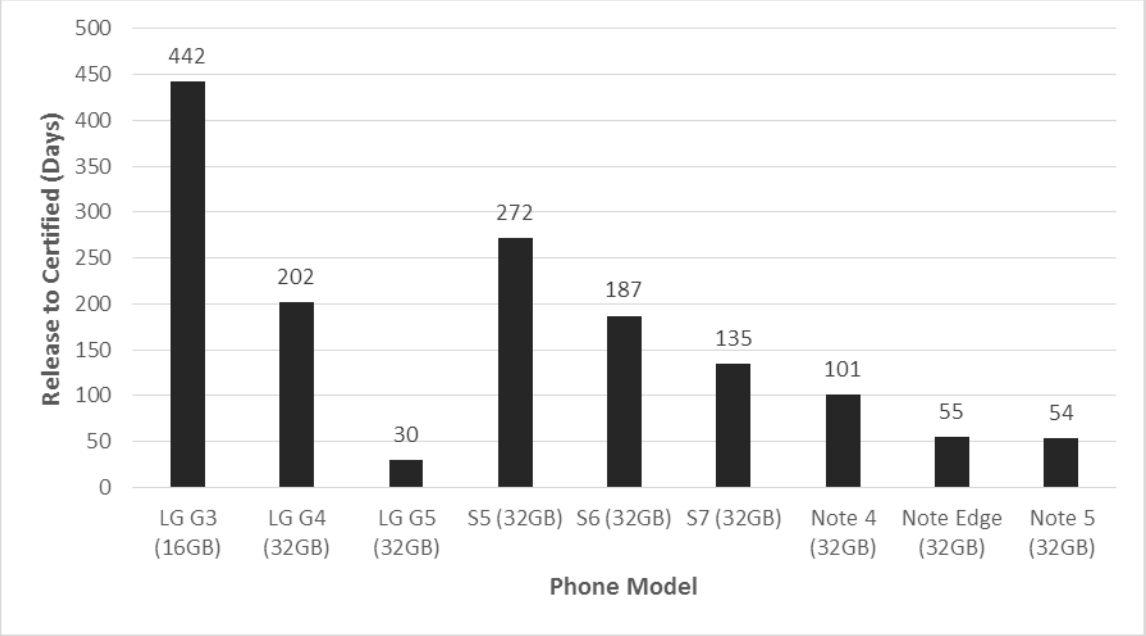


All iPhones that are currently produced and certified (green columns), with the exception of the SE 16 and 64GB, are all still currently produced as of July 15, 2017. Phones currently in production have been certified for 131 days as of July 15, 2017.

2. Android Data

The amount of time necessary for various Android devices to become certified on the DoDIN APL is demonstrated in Figure 16. As shown, certification times appear to be getting better, leading to an increased amount of time that phone models will be in production and DoDIN APL certified.

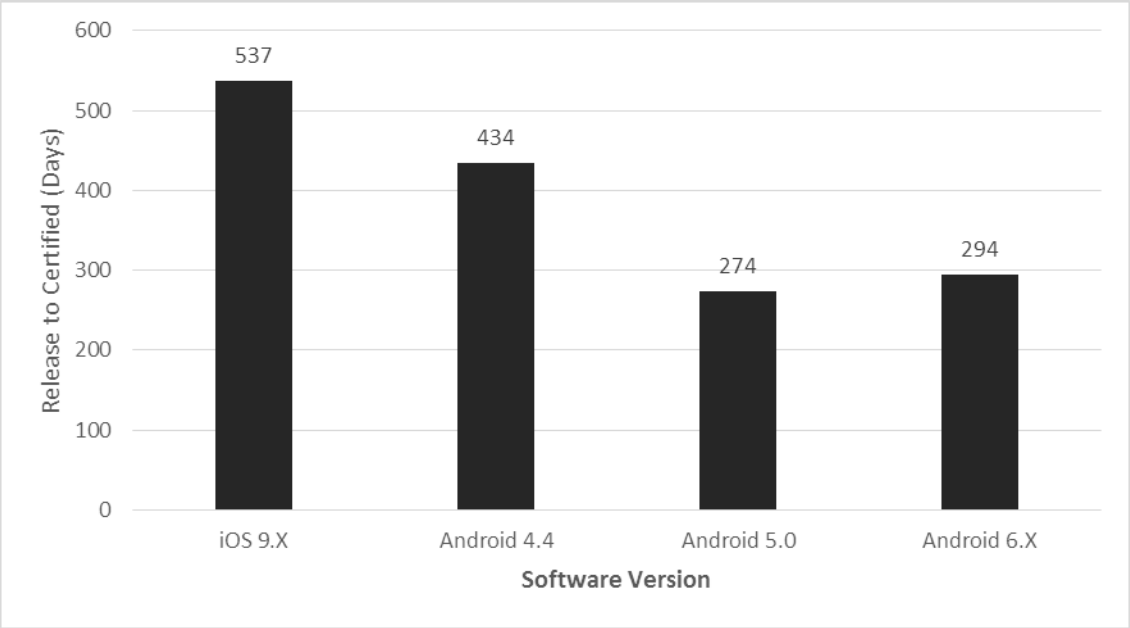
Figure 16. Android Phones DoDIN APL Certification Time



3. Software Data

When a phone is certified on the DoDIN APL, a corresponding software package and version is also certified. The timelines from certain versions release to verification is shown in Figure 17. This is particularly important from a security perspective since outdated software may have several vulnerabilities and the patches/fixes to those vulnerabilities may not be DoDIN APL approved.

Figure 17. Software DoDIN APL Certification Time



D. AIRBORNE AND MARITIME FIXED STATION JOINT TACTICAL RADIO SYSTEM

AMF JTRS represents one of two comparable ACAT I programs with data available through the Defense Acquisition Management Information Retrieval (DAMIR). AMF JTRS was chosen due to its similarity in size and capability when compared to a handheld commercial mobile device and its similar capabilities in being able to transmit various types of data (voice, text, video, position, etc.). For our purposes, cost and performance were not included since the timeline of production from Milestone B to FRP is being compared against commercial mobile device development timelines. The timeline from inception of AMF JTRS to the current estimated completion dates is shown in Figure 18. All baseline schedule targets were missed, with most having delays of 10+ years.

Figure 18. Original and Current Schedule Estimates for AMF JTRS.
Source: Schedule for AMF JTRS (PNO: 421) (DAMIR) (2017a).

Schedule Events				
Events	**SAR Baseline Development Estimate**	**Current APB Development Objective/Threshold**		**Current Estimate**
Milestone B Decision	Dec 2007	Mar 2008	Mar 2008	Mar 2008
Contract Award	Feb 2008	Nov 2021	May 2022	Oct 2019
Milestone C Decision	Nov 2011	Oct 2022	Apr 2023	Mar 2022
FRP	Jul 2014	Jun 2023	Dec 2023	Oct 2023
IOC	Aug 2014	Apr 2026	Oct 2026	Jul 2024

The scheduled slippage from the original estimated completion date to the current completion date or estimate completion date are shown in Table 8. AMF JTRS has been plagued by schedule overruns due to a lack of the required technology to meet requirements, and it is generally accepted to be about 10 years behind schedule.

Table 8. AMF JTRS Schedule Overages
Adapted from Schedule for AMF JTRS (PNO: 421) (DAMIR) (2017a).

Events	**Schedule Slippage (Time between SAR Baseline Development Estimate and Current Estimate)**
MS B Decision	3 months
Contract Award	10 years, 7 months
Milestone C Decision	10 years, 4 months
FRP	9 years, 3 months
IOC	9 years, 11 months

E. HMS

Handheld, Manpack, and Small Form Fit (HMS) is the other comparable ACAT I system with data available through DAMIR. For data purposes, only the AR/PRC-154 Rifleman Radio was chosen because the AN/PRC-155 Manpack does not compare to a traditional commercial mobile device. The original estimated scheduling and current schedule for the AN/PRC 154 is displayed in the table located in Figure 19.

Figure 19. Original and Current Schedule Estimate for HMS AN/PRC-154
Adapted from Schedule for HMS (PNO: 385) (DAMIR) (2017b).

Events	SAR Baseline Development Estimate	Current APB Development Objective/Threshold		Current Estimate
Milestone B Decision	Apr 2004	May 2004	May 2004	May 2004
Contract Award	Jul 2004	Jul 2004	Jul 2004	Jul 2004
Milestone C Decision	May 2011	Jun 2011	Jun 2011	Jun 2011
IOT&E: AN/PRC-154	Nov 2011	Nov 2011	Nov 2011	Nov 2011
IOC: AN/PRC-154	Jan 2012	Jul 2012	Jul 2012	Jul 2012
FRP Decision Review	May 2012	Apr 2018	Oct 2018	TBD[1]

The schedule slippages for the HMS AN/PRC154 are shown in Table 9. Development of the AN/PRC-154 has been good through the first phases of the program, but the FRP decision review has been pushed out several years past the original estimated date.

Table 9. HMS Schedule Overages.
Adapted from Schedule for HMS (PNO: 385) (DAMIR) (2017b).

Events	Schedule Slippage (Time between SAR Baseline Development Estimate and Current Estimate)
MS B Decision	1 month
Contract Award	0 months
Milestone C Decision	1 month
IOT&E: AN/PRC-154	0 months
IOC: AN/PRC-154	6 months
FRP Decision Review	5 years, 11 months (based on Objective)

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DISCUSSION

A. STANDARDS-BASED VS. REQUIREMENTS-BASED APPROACH

Secretary of Defense William Perry issued a memo in 1994 also known as "The Perry Memo" that declared "the problem is rooted in the requirements determination phase of the acquisition cycle" and encouraged greater use of standards (Perry, 1994, para. 17). Traditional DOD acquisitions implements a requirements-based approach that prescribes to user requirements specified up-front in approved documents, adheres to the JCIDS requirements process, and implements individual service processes for requirements (Nidiffer, Miller, & Carney, 2014). Nidiffer et al. (2014) identified issues that arose from the requirements-based approach that included outdated requirements from early in the process, little support for COTS solutions, and lack of coordination between users, acquirers, and developers. DAU (2013) encouraged a standards-based approach called the modular open systems approach (MOSA) that was "defined as an acquisition and design strategy consisting of a technical architecture that adopts open standards and supports a modular, loosely coupled and highly cohesive system structure" (p. 310). MOSA benefits the DOD through high interoperability by only setting minimum standards, resulting in increased participation and competition among vendors and higher innovation, technology refresh, and cost savings (DAU, 2013). The warfighter also benefits from lower learning curves through the use of familiar systems, higher interchangeability, and lower sustainment costs (DAU, 2013).

Open standards is a key component to MOSA and is defined through the DOD Information Technology Standards Registry (DISR) which "mandates the minimum set of standards and guidelines for the acquisition of all DOD systems that produce, use, or exchange information" ("Systems Engineering: Modular Open Systems Approach," 2017, para. 3).

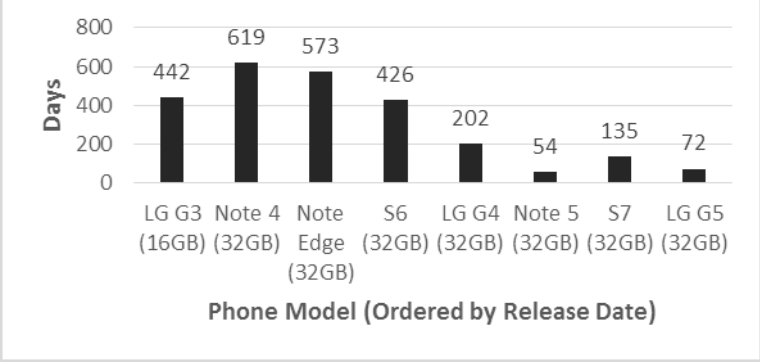
Additional standards include the Commercials Solutions for Classified (CSfC) and DOD Information Network Approved Products List (DoDIN APL), which aim to facilitate interoperability, information assurance, and classified functions. CSfC and

DoDIN APL are important and recognized standards endorsed by current certification authorities on federal and defense IT systems.

B. CSFC AND DODIN APL

CSfC provides classified capabilities to the DOD for classified systems, allowing the DOD to leverage newer and more modern hardware and software, while increasing flexibility and lowering future costs. CSfC capability packages can be customized with CSfC products, such as MDM for device management and IPSec VPN for access to private USMC networks. By choosing DoDIN APL products, we can be assured that these products have already been certified by the Joint Interoperability Test Command (JITC) and meets information assurance and Net Ready KPP requirements to shorten the overall acquisition cycle (DISA, 2017). Devices approved on the DoDIN APL are also approved to operate on the Global Information Grid (GIG) (DISA, 2017). Since CSfC focuses only on providing classified capabilities, certain models of mobile devices may not be on both the DoDIN APL and CSfC lists. As demonstrated in Figure 20, between different brands and models the certification time for mutual inclusion in both the CSfC and DoDIN APL lists are getting significantly shorter from the mobile devices' original release date. While DoDIN APL does not state a target goal for a timeline for certification devices, CSfC targets 90 days through the use of NIAP, and NIAP certification timelines cannot exceed 180 days (NIAP, 2014).

Figure 20. Time to Certification for both CSfC and APL (Ordered by Release Date)



1. Android vs. Apple

For the purposes of this thesis, we defined “mobile devices” as smartphones and tablets using the Android and Apple operating systems. As of July 2017, the latest Apple devices that are both DoDIN APL and CSfC certified and approved are the iPhone 6 and 6 Plus with 16Gb and 64GB storage options. These devices have an official manufacturer end date of Sept 7, 2016, indicating that the devices are approximately 11 months out of production at the time of this thesis. There are several iPhones currently being produced on the DoDIN APL (6S, 6S Plus, SE, 7, & Plus), but none of those specific devices have been also certified by CSfC. The NIAP is currently evaluating iOS 10.2 for various iPhones and iPads, but does not list which specific devices are being evaluated. This certification process was started on March 10, 2017, exceeding the target certification timeline of 90 days and is closely approaching the maximum allowed timeline of 180 days.

Currently, several Android devices, including the LG G5 and Samsung Galaxy S7, are on the DoDIN APL and CSfC. The inclusion time of Android devices on the DoDIN APL and CSfC averaged 72 and 135 days, respectively, after it had been in production for about 16 months. Due to an increased number of phone models/lines (LG G Series, Samsung Note and S series), it appears that there are more opportunities to certify Android devices than there are Apple devices. Based on past data, it also appears that Android certification is faster than Apple certification.

Based on the DoDIN APL and CSfC standards, Android devices are currently the only viable option due to its inclusion on both lists. Apple devices may be available for consideration in the near future. USMC must determine its desired procurement timeline with device functionalities and features between Android and Apple products. Regardless of procurement choice, the Life Cycle Sustainment Plan (LCSP) will be a shared consideration for mobile devices and must be tailored in the context of the standards.

2. Life Cycle Sustainment Plan

The LCSP for mobile devices will focus on operational supportability to include design, maintenance, and disposal (USD(AT&L), 2017). Based on the data gathered on

mobile device release dates and CSfC & DoDIN APL certification dates, prior generations of mobile devices with current operating systems would allow significant cost savings with a minimal impact on capability. MDM through the CSfC offers a wide spectrum of capabilities to update all devices through remote means, for example: policy enforcement of restrictions and limitations, such as OS platforms and application downloads; security measures for lost/stolen phones, such as device lock and remote wipe; containerization to separate personal from business content; and application management, such as patches/fixes, and backup/restore (Basso & Redman, 2012). When replacing mobile devices with the next generation, there may be no need to recertify for interoperability if replacement devices are on the DoDIN APL as certified by JITC (DISA, 2017). Mobile devices outside of their useful life will be considered excess personal property and will be exchanged/sold or disposed of in accordance with the U.S. General Services Administration (GSA)'s Personal Property Disposal Guide: "When replacing personal property with similar items, the exchange/sale authority provides for the value of the old items to be used to reduce the cost of the replacement item either by exchange (trade-in) or sale and use of the proceeds in the acquisition of the replacement item" (GSA, 2017b, p. 25). However, before considering device choice and LCSP, close coordination must first be conducted between the primary organizations within Marine Corps acquisitions.

C. MARINE CORPS ACQUISITIONS

Marine Corps Combat Development Center (MCCDC) is responsible for the development of "fully integrated Marine Corps warfighting capabilities; including doctrine, organization, training and education, materiel, leadership, personnel, and facilities (DOTMLPF), to enable the Marine Corps to field combat-ready forces" (USMC, 2010, p. 2). Marine Corps Systems Command (MCSC) is the acquisition arm of the Marine Corps and is the "Marine Corps materiel developing agent" (USMC, 2010, p. 3). Marine Corps Operational Test and Evaluation Activity (MCOTEA) conducts independent operational test functions for the Marine Corps (USMC, 2010). The three listed organizations play primary roles in the USMC acquisition process and are collectively known as the "Triad" (USMC, 2010). Although MCCDC takes the lead in

requirements development, MCSC in acquisition management, and MCOTEA in operational test & evaluation, early and continuous coordination between all three organizations are made throughout the entire USMC acquisition process (USMC, 2010).

Although the Marine Corps RCO is still in its infancy and is drafting its charter at the time of this thesis, we see great potential in its agile structure and position under MCCDC to help accelerate the acquisition of mobile devices. The Marine Corps RCO's vision is to "rapidly develop and deliver operational prototypes" to limited units in the operating forces to "assess their value more quickly than current processes support" and facilitate "potential transition to the formal acquisition process" (United States Marine Corps Rapid Capabilities Office [USMC RCO], 2016, p. 4). Rapid testing of operational prototypes of mature technology reduces programmatic risk by quickly determining viability and identifying issues early in the process before committing to a full program of record (Hencke, 2014). Operational testing through the Marine Corps RCO will also identify opportunities and challenges for future integration in DOTMLPF.

D. COMPARISON OF IT ACQUISITION STRATEGIES

Since our proposed strategy enters the DAS at Milestone C due to the high technology maturity and prior assessment, we will substitute the proposed strategy's "Milestone B to C" for the length of time the Marine Corps RCO would take to purchase and assess mobile devices through its RCO process, or 12 months (USMC RCO, 2016)

Table 10. Comparison of IT Acquisition Strategies.

Program/Strategy	Milestone B to C	Milestone C to IOC
JTRS	168 months	28 months
HMS	85 months	13 months
Proposed Strategy	12 months	13 months

Once devices have been assessed and deemed operationally viable by the RCO, next generation devices from the same product line (i.e. G5 and G6) could go through an accelerated testing and operational evaluation step once put on both the CSfC and DoDIN APL. The similarities between phones of the same product line should allow the

elimination of some required testing, since the devices share many common characteristics, putting a larger emphasis on testing the impact of changes between generations. This should allow the USMC to purchase devices within 6–9 months of release, assuming that the current trend of CSfC and DoDIN APL certification continues to be shortened and occurs within 90 days.

V. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

Our research aimed to answer two questions: 1. Do current acquisition strategies allow for cost effective acquisition of COTS mobile devices before they become obsolete?; and 2. How can we rapidly procure mobile devices while meeting DOD requirements? Current acquisition strategies are being out-paced by the increasing speed of mobile device technology due to the requirements-based approach that prescribes to user requirements specified up-front in approved documents, adheres to the JCIDS requirements process, and implements individual service processes for requirements (Nidiffer et al., 2014). Rapid procurement of mobile devices may be possible with a standards-based approach through MOSA that sets minimum open standards for maximizing interoperability, competition, and cost savings (DAU, 2013).

Rapid capabilities units do not provide additional "capabilities" that are outside the purview of a program manager. Due to the complexity of the DAS and the uniqueness of each product and circumstances, "MDAs have full latitude to tailor programs in the most effective and efficient structure possible, to include eliminating phases and combining or eliminating milestones and decision points, unless constrained by statute" (USD(AT&L), 2017, p. 9). For reasons outside the scope of this thesis, program managers have limitations that are temporarily resolved by rapid capabilities units to facilitate rapid acquisition of emerging technology, such as the Marine RCO. As an optional method, the Marine RCO may provide rapid testing of operational prototypes of mature technology to reduce programmatic risk by quickly determining viability and identifying issues early in the process before committing to a full program of record (Hencke, 2014).

B. RECOMMENDED COURSE OF ACTION

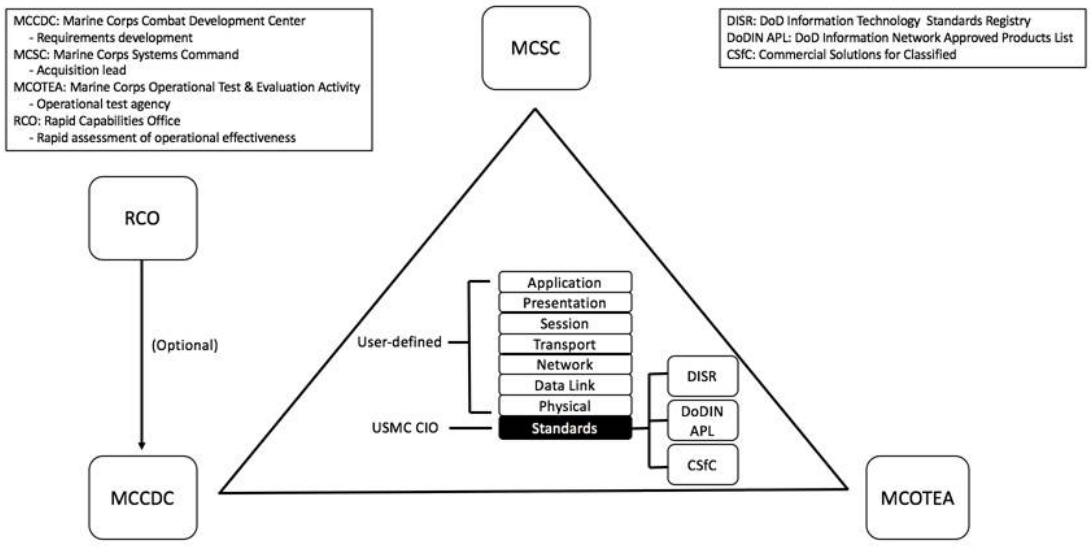
We recommend using MOSA as a standards-based approach to set minimum open standards from DISR for products on the DoDIN APL, and CSfC. By choosing mobile devices and products which are already DoDIN APL and CSfC certified, we can

accelerate meeting the information assurance and interoperability requirements and ultimately, the procurement of those devices. Due to the technology maturity, low development effort associated with COTS devices, and flexibility given to the MDAs to tailor their programs, the DAS may then be entered at Milestone C to go into operational testing and rapid fielding to the warfighter.

The early and continuous coordination between the "Triad", with MCCDC as the owner of requirements development, MCSC as the acquisitions lead, and MCOTEA as the operational test agency is shown in Figure 21. The acquisition strategy of the "Triad" revolves around the standards-based approach using DISR, DoDIN APL, and CSfC standards with oversight from the USMC Chief Information Officer (CIO) (US Congress, 1996). All other layers above the standards layer (ie. OSI model) are considered user-defined. To best be able to take advantage of the MOSA strategy for acquisitions, the operational community and the USMC acquisition community (MCCDC, MARCORSYSCOM and MCOTEA) should establish a liaison team to enable rapid application and adoption of MOSA guidelines. This has the capability to enable rapid procurement of mobile devices and any other type of system that could benefit from a MOSA type approach.

As an optional method, the Marine RCO could procure operational prototypes, which met the minimum standards, using OTA to identify opportunities and challenges for future integration in DOTMLPF, thereby reducing downside risk by verifying a proof of concept before committing to a full program of record.

Figure 21. USMC COTS Mobile Device Acquisition Strategy



C. LIMITATIONS

Unreliability of data for ACAT II and III programs to determine cost, schedule, and performance caused us to focus on comparing our proposed mobile device acquisition strategy with similar ACAT I programs (GAO, 2015b). According to GAO (GAO, 2015b), there is no requirement for ACAT II and III programs to publish their data on Defense Acquisition Management Information Retrieval (DAMIR) system, so their findings consisted of "widespread data entry issues and missing data" and "inconsistent identification of current ACAT II and III programs" (p. 6).

Although there has been significant lag period between the production of a commercial mobile device and the CSfC & DoDIN APL certification process, the trend over time demonstrates that the certification time is getting faster, and in some cases, under 60 days. The tradeoff of the DOD procuring prior generation mobile devices vice emergent from vendors is the loss of the immediate use the latest technology over increased reliability over time.

D. RECOMMENDATIONS FOR FUTURE RESEARCH

In this research, we proposed a strategy that operated within the current confines of federal regulations and policies. A recommendation for future research is to seek ways to shorten the acquisition process for mobile devices through policy changes and to conduct a cost/benefit analysis to compare the proposed and current policy changes. Another recommendation for future research is to analyze the JCIDS and/or PPBE processes to seek further efficiencies, reductions, or policy changes.

APPENDIX A. COMMERCIAL CELL PHONE DATA

Phone Model	Release Date	Production End Date	Cost (Release)	Cost (2017)	RAM	Max Processor	Processor Speed (GHZ)
iPhone							
iPhone (4GB)	6/29/2007	9/5/2007	499	592	128MB	412MHz	0.412
8GB	6/29/2007	6/9/2008	399	474	128MB	412MHz	0.412
16GB	2/5/2008	6/9/2008	499	586	128MB	412MHz	0.412
3G (8 GB)	7/11/2008	6/7/2010	499	582	128MB	412MHz	0.412
16 GB	7/11/2008	6/8/2009	599	698	128MB	412MHz	0.412
3GS (8GB)	6/8/2010	9/12/2012	499	563	128MB	600MHz	0.6
16 GB	6/19/2009	6/7/2010	599	687	128MB	600MHz	0.6
32 GB	6/19/2009	6/7/2010	699	802	128MB	600MHz	0.6
4 (16GB)	6/24/2010	10/11/2011	649	731	512MB	800MHz	0.8
32GB	6/24/2010	10/11/2011	749	844	512MB	800MHz	0.8
8GB	10/4/2011	9/10/2013	549	605	512MB	800MHz	0.8
4S (8GB)	9/10/2013	9/14/2014	450	479	512MB	1GHz (Dual Core)	2
16GB	10/14/2011	9/10/2013	649	715	512MB	1GHz (Dual Core)	2
32GB	10/14/2011	9/12/2012	749	825	512MB	1GHz (Dual Core)	2
64GB	10/14/2011	9/12/2012	849	935	512MB	1GHz (Dual Core)	2
5 (16GB)	9/21/2012	9/10/2013	649	703	1GB	1.3GHz (Dual Core)	2.6
32GB	9/21/2012	9/10/2013	749	812	1GB	1.3GHz (Dual Core)	2.6
64GB	9/21/2012	9/10/2013	849	920	1GB	1.3GHz (Dual Core)	2.6
5S (16GB)	9/20/2013	3/21/2016	649	691	1GB	1.3GHz (Dual Core)	2.6
32GB	9/20/2013	3/21/2016	749	798	1GB	1.3GHz (Dual Core)	2.6
64GB	9/20/2013	9/9/2014	849	904	1GB	1.3GHz (Dual Core)	2.6
5C (8GB)	9/9/2014	9/9/2015	450	471	1GB	1.3GHz (Dual Core)	2.6
16GB	9/20/2013	9/9/2014	549	585	1GB	1.3GHz (Dual Core)	2.6
32GB	9/20/2013	9/9/2014	649	691	1GB	1.3GHz (Dual Core)	2.6
6 (16GB)	9/19/2014	9/7/2016	649	679	1GB	1.4GHz (Dual Core)	2.8
64GB	9/19/2014	9/7/2016	749	784	1GB	1.4GHz (Dual Core)	2.8
128GB	9/19/2014	9/15/2015	849	888	1GB	1.4GHz (Dual Core)	2.8
6 Plus (16GB)	9/19/2014	9/7/2016	749	784	1GB	1.4GHz (Dual Core)	2.8
64GB	9/19/2014	9/7/2016	849	888	1GB	1.4GHz (Dual Core)	2.8
128GB	9/19/2014	9/9/2015	949	993	1GB	1.4GHz (Dual Core)	2.8
6S (16GB)	9/25/2015	9/7/2016	649	667	2GB	1.85GHz (Dual Core)	3.7
32GB	9/7/2016	5/31/2017	549	555	2GB	1.85GHz (Dual Core)	3.7
64GB	9/25/2015	9/7/2016	749	770	2GB	1.85GHz (Dual Core)	3.7
128GB	9/25/2015	5/31/2017	849	873	2GB	1.85GHz (Dual Core)	3.7
6S Plus (16GB)	9/25/2015	9/7/2016	749	770	2GB	1.85GHz (Dual Core)	3.7
32GB	9/7/2016	5/31/2017	649	656	2GB	1.85GHz (Dual Core)	3.7
64GB	9/25/2015	9/7/2016	849	873	2GB	1.85GHz (Dual Core)	3.7
128GB	9/25/2015	5/31/2017	949	976	2GB	1.85GHz (Dual Core)	3.7
SE (16GB)	3/31/2016	3/21/2017	399	407	2GB	1.85GHz (Dual Core)	3.7
32GB	3/21/2017	5/31/2017	399	400	2GB	1.85GHz (Dual Core)	3.7

64GB	3/31/2016	3/21/2017	499	508	2GB	1.85GHz (Dual Core)	3.7
128GB	3/21/2017	5/31/2017	499	500	2GB	1.85GHz (Dual Core)	3.7
7 (32GB)	9/16/2016	5/31/2017	649	656	2GB	2.3GHz (Quad Core)	9.2
128GB	9/16/2016	5/31/2017	749	757	2GB	2.3GHz (Quad Core)	9.2
256GB	9/16/2016	5/31/2017	849	858	2GB	2.3GHz (Quad Core)	9.2
7 Plus (32GB)	9/16/2016	5/31/2017	769	777	3GB	2.3GHz (Quad Core)	9.2
128GB	9/16/2016	5/31/2017	869	878	3GB	2.3GHz (Quad Core)	9.2
256GB	9/16/2016	5/31/2017	969	979	3GB	2.3GHz (Quad Core)	9.2

Optimus G

LG G (16GB)	9/19/2012		549	595	2GB	1.5GHz (Quad Core)	6
Optimus G Pro (32GB)	5/10/2013		600	643	2GB	1.7GHz (Quad Core)	6.8
LG G2 (32GB)	9/12/2013		630	671	2GB	2.26GHz (Quad Core)	9.04
LG G2 Pro (32GB)	3/14/2014		650	686	3GB	2.26GHz (Quad Core)	9.04
LG G3 (16GB)	5/28/2014		600	631	2GB	2.5GHz (Quad Core)	10
32GB	5/28/2014		700	737	3GB	2.5GHz (Quad Core)	10
LG G4 (32GB)	4/29/2015		550	570	3GB	1.82GHz (Hexa Core)	9.4
LG G5 (32GB)	4/23/2016		625	636	4GB	2.15GHz (Quad Core)	7.46
LG G6 (32GB)	3/10/2017		650	651	4GB	2.34GHz (Quad Core)	9.06
64GB	3/10/2017		700	702	4GB	2.34GHz (Quad Core)	9.06

Samsung (S)

S (8GB)	6/4/2010		600	677	512MB	1GHz	1
S2 (16GB)	5/2/2011		699	776	1GB	1.2 GHz (Dual core)	2.4
S3 (16GB)	5/29/2012		599	653	2GB	1.5 GHz (Quad core)	5.6
32GB	5/29/2012		649	707	2GB	1.4 GHz (Quad core)	5.6
S4 (16GB)	4/23/2013		640	686	2GB	1.6 GHz (Octa core)	11.2
S5 (32GB)	4/11/2014		650	685	2GB	1.9 GHz (Octa core)	12.8
S6 (32GB)	4/10/2015		600	622	3GB	2.1 GHz (Octa core)	14.4
64GB	4/10/2015		700	725	3GB	2.1 GHz (Octa core)	14.4
128GB	4/10/2015		800	829	3GB	2.1 GHz (Octa core)	14.4
S7 (32GB)	3/12/2016		670	683	4GB	2.3 GHz (Octa core)	15.6
S8	4/21/2017		750	750	4GB	2.45 GHz (Octa core)	17.4

Samsung (Note)

Note (32GB)	10/28/2011				1GB	1.4GHz (Dual core)	2.8
Note 2 (64GB)	9/27/2012		700	758	2GB	1.6GHz (Quad core)	6.4
Note 3 (64GB)	9/25/2013		699	744	3GB	2.3GHz (Quad core)	9.2
Note 3 Neo (16GB)	2/1/2014		800	846	2GB	1.7GHz (Hexa core)	8.6
Note 4 (32GB)	9/29/2014		600	628	3GB	1.9 GHz (Octa core)	12.8
Note Edge (32GB)	11/14/2014		840	877	3GB	2.7GHz (Quad core)	10.8
Note 5 (32GB)	8/21/2015		700	721	4GB	2.1GHz (Octa core)	14.4
64GB	8/21/2015		800	824	4GB	2.1GHz (Octa core)	14.4

APPENDIX B. DODIN APL DEVICES

Phone Model	Release Date	Production End Date	Certification Date	Days from Release to Certified	Produced and Certified
iPhone					
4S (8GB)	9/10/2013	9/14/2014	3/6/2017	1273	-904
4S (16GB)	10/14/2011	9/10/2013	3/6/2017	1970	-1273
4S (32GB)	10/14/2011	9/12/2012	3/6/2017	1970	-1636
4S (64GB)	10/14/2011	9/12/2012	3/6/2017	1970	-1636
5 (16GB)	9/21/2012	9/10/2013	3/6/2017	1627	-1273
5 (32GB)	9/21/2012	9/10/2013	3/6/2017	1627	-1273
5 (64GB)	9/21/2012	9/10/2013	3/6/2017	1627	-1273
5S (16GB)	9/20/2013	3/21/2016	3/6/2017	1263	-350
5S (32GB)	9/20/2013	3/21/2016	3/6/2017	1263	-350
5S (64GB)	9/20/2013	9/9/2014	3/6/2017	1263	-909
5C (8GB)	9/9/2014	9/9/2015	3/6/2017	909	-544
5C (16GB)	9/20/2013	9/9/2014	3/6/2017	1263	-909
5C (32GB)	9/20/2013	9/9/2014	3/6/2017	1263	-909
6 (16GB)	9/19/2014	9/7/2016	3/6/2017	899	-180
6 (64GB)	9/19/2014	9/7/2016	3/6/2017	899	-180
6 (128GB)	9/19/2014	9/15/2015	3/6/2017	899	-538
6 Plus (16GB)	9/19/2014	9/7/2016	3/6/2017	899	-180
6 Plus (64GB)	9/19/2014	9/7/2016	3/6/2017	899	-180
6 Plus (128GB)	9/19/2014	9/9/2015	3/6/2017	899	-544
6S (16GB)	9/25/2015	9/7/2016	3/6/2017	528	-180
6S (32GB)	9/7/2016	7/15/2017	3/6/2017	180	131
6S (64GB)	9/25/2015	9/7/2016	3/6/2017	528	-180
6S (128GB)	9/25/2015	7/15/2017	3/6/2017	528	131
6S Plus (16GB)	9/25/2015	9/7/2016	3/6/2017	528	-180
6S Plus (32GB)	9/7/2016	7/15/2017	3/6/2017	180	131
6S Plus (64GB)	9/25/2015	9/7/2016	3/6/2017	528	-180
6S Plus (128GB)	9/25/2015	7/15/2017	3/6/2017	528	131
SE (16GB)	3/31/2016	3/21/2017	3/6/2017	340	15
SE (32GB)	3/21/2017	7/15/2017	3/6/2017	-15	131
SE (64GB)	3/31/2016	3/21/2017	3/6/2017	340	15
SE (128GB)	3/21/2017	7/15/2017	3/6/2017	-15	131
7 (32GB)	9/16/2016	7/15/2017	3/6/2017	171	131
7 (128GB)	9/16/2016	7/15/2017	3/6/2017	171	131
7 (256GB)	9/16/2016	7/15/2017	3/6/2017	171	131
7 Plus (32GB)	9/16/2016	7/15/2017	3/6/2017	171	131
7 Plus (128GB)	9/16/2016	7/15/2017	3/6/2017	171	131
7 Plus (256GB)	9/16/2016	7/15/2017	3/6/2017	171	131

Optimus G

LG G3 (16GB)	5/28/2014		8/13/2015	442	
LG G4 (32GB)	4/29/2015		11/17/2015	202	
LG G5 (32GB)	4/23/2016		5/23/2016	30	

Samsung (S)

S5 (32GB)	4/11/2014		1/8/2015	272	
S6 (32GB)	4/10/2015		10/14/2015	187	
S7 (32GB)	3/12/2016		7/25/2016	135	

Samsung (Note)

Note 4 (32GB)	9/29/2014		1/8/2015	101	
Note Edge (32GB)	11/14/2014		1/8/2015	55	
Note 5 (32GB)	8/21/2015		10/14/2015	54	

Software

iOS 9.X	9/16/2015		3/6/2017	537	
Android 4.4	10/31/2013		1/8/2015	434	
Android 5.0	11/12/2014		8/13/2015	274	
Android 6.X	10/5/2015		7/25/2016	294	

APPENDIX C. CSFC DEVICES

Phone Model	Release Date	Production End Date	Certification Date	Days from Release to Certified	Produced and Certified
iPhone					
5S (16GB)	9/20/2013	3/21/2016	1/28/2016	860	53
5S (32GB)	9/20/2013	3/21/2016	1/28/2016	860	53
5S (64GB)	9/20/2013	9/9/2014	1/28/2016	860	-506
6 (16GB)	9/19/2014	9/7/2016	1/28/2016	496	223
6 (64GB)	9/19/2014	9/7/2016	1/28/2016	496	223
6 (128GB)	9/19/2014	9/15/2015	1/28/2016	496	-135
6 Plus (16GB)	9/19/2014	9/7/2016	1/28/2016	496	223
6 Plus (64GB)	9/19/2014	9/7/2016	1/28/2016	496	223
6 Plus(128GB)	9/19/2014	9/9/2015	1/28/2016	496	-141
Optimus G					
LG G3 (16GB)	5/28/2014		3/30/2015	306	
LG G4 (32GB)	4/29/2015		7/1/2015	63	
LG G5 (32GB)	3/12/2016		4/14/2016	33	
LG G6 (32GB)	3/10/2017		5/2/2017	53	
Samsung (S)					
S6 (32GB)	4/10/2015		6/9/2016	426	
S7 (32GB)	3/12/2016		5/25/2016	74	
S8 (64GB)	4/21/2017		6/15/2017	55	
Samsung (Note)					
Note 4 (32GB)	9/29/2014		6/9/2016	619	
Note Edge (32GB)	11/14/2014		6/9/2016	573	
Note 5 (32GB)	8/21/2015		10/13/2015	53	
Software					
iOS 9.2	12/8/2015		1/28/2016	42397	
Android 5.0.1	12/2/2014		3/30/2015	42093	
Android 5.1	3/9/2015		7/1/2015	42186	
Android 5.1.1	4/21/2015		10/13/2015	42290	
Android 6.0.1	12/7/2015		4/14/2016	42474	
Android 7.0	8/22/2016		6/15/2017	42901	

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Agre, J., Gordon, K. D., & Vassiliou, M. S. (2013). *Commercial technology at the tactical edge*. Alexandria, VA: Institute for Defense Analysis. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA587552

Anderson, S., & Rutherford, H. (2013). DOD's Commercial Mobile Device Implementation Plan. Retrieved from http://www.doncio.navy.mil/mobile/ContentView.aspx?ID=4534&TypeID=21

Alastruey, J., Briz, J. L., Ibanez, P., & Vinals, V. (2006). Software demand, hardware supply, *IEEE Micro, 26*(4), 72–82

Arellano, R. (2015). *Analysis of rapid acquisition processes to fulfill future urgent needs* (Master's thesis). Retrieved from http://hdl.handle.net/10945/47836

Aten, K. (2013). *Defense acquisition and the case of the joint capabilities technology demonstration office: Ad hoc problem solving as a mechanism for adaptive change* (Technical Report). Monterey, CA: Naval Postgraduate School. Retrieved from http://calhoun.nps.edu/bitstream/handle/10945/34565/NPS-AM-13-C10P01R014-043.pdf?sequence=1

Basso, M., & Redman, P. (2012). *Critical capabilities for mobile device management*. Gartner. Retrieved from http://www.tsd.ac.uk/en/media/uniweb/content/documents/departments/informationservices/studentinformation/airwatch_report.pdf

Bouchoux, D. E. (2015). *Patent law of paralegals.* Moorpark, CA: Content Technologies. Retrieved from https://books.google.com/books?id=tndcobutkEkC&pg=PT117&lpg=PT117&dq=the+BlackBerry+was+crucial+for+national+security+given+the+large+number+of+government+users&source=bl&ots=caXIlHPhQF&sig=obgc7O8CFV3XPYy3G7Kwj4kVyZQ&hl=en&sa=X&ved=0ahUKEwiM9JvE96HTAhXmqVQKHZYvC6YQ6AEIIzAB#v=onepage&q=the%20BlackBerry%20was%20crucial%20for%20national%20security%20given%20the%20large%20number%20of%20government%20users&f=false

Browne, M. (2016). Marine Corps Systems Command: Equipping our Marines. Retrieved from http://www.marcorsyscom.marines.mil/News/Press-Release-Article-Display/Article/849456/new-program-will-give-dismounted-marines-secure-smart-devices/

Brzoska, M. (2006). *Trends in global military and civilian research and development (R&D) and their changing interface*. Hamburg, DE: University of Hamburg. Retrieved from http://ifsh.de/pdf/aktuelles/india_brzoska.pdf

Bureau of Labor Statistics. (2017). Consumer Price Index. Retrieved from https://data.bls.gov/pdq/SurveyOutputServlet?request_action=wh&graph_name=CU_cpibrief

Carter, A. (2016, May 11). The "X" is for experimental. Retrieved from https://medium.com/@SecDef/the-x-is-for-experimental-3c9438e76214#.dty43j9ju

Chairman of the Joint Chiefs of Staff. (2005). *Rapid validation and resourcing of joint urgent operational needs (JUONS) in the year of execution*. Washington, DC: White House.

Cheng, J. (2014) BlackBerry 10 passes DISA's 'full operational' tests. Retrieved from https://defensesystems.com/articles/2014/04/01/blackberry-disa-foc-designation.aspx

Chief Information Office (CIO) Council. (2012a). Bring your own device: a toolkit to support federal agencies implementing bring your own device (BYOD) Programs. Retrieved from https://cio.gov/wp-content/uploads/downloads/2012/09/byod-toolkit.pdf

Chief Information Office (CIO) Council. (2012b). *Government use of mobile technology: Barriers, opportunities, and gap analysis*. White House: CIO Council. Retrieved from https://cio.gov/wp-content/uploads/downloads/2012/12/Government_Mobile_Technology_Barriers_Opportunities_and_Gaps.pdf

Chief Information Office (CIO) Council. (2013a). Adoption of commercial mobile applications within the Federal Government. Retrieved from https://cio.gov/wp-content/uploads/downloads/2013/05/Commercial-Mobile-Application-Adoption-DGS-Milestone-5.4.pdf

Chief Information Office (CIO) Council. (2013b). *Government mobile and wireless security baseline*. White House: CIO Council. Retrieved from https://cio.gov/wp-content/uploads/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf

Copeland, D. (2011) Game Changer: Nett Warrior provides cutting-edge technologies for situational awareness and communications. Retrieved from http://asc.army.mil/docs/pubs/alt/2011/3_JulAugSep/articles/22_Game_Changer_201103.pdf

Defense Acquisition Management Information Retrieval (DAMIR). (2017a). Schedule for AMF JTRS (PNO: 421) from SAR Dec 2016. Retrieved from https://ebiz.acq.osd.mil/DAMIR/PurviewNew/PurviewDefault.aspx?progId=150960&subProgId=2478&subType=SAR&source=urn%3aus%3amil%3aosd%3aacq%3adamir%3asar&effDate=12%2f25%2f2016&subId=166853&controlToLoad=65

Defense Acquisition Management Information Retrieval (DAMIR). (2017b). Schedule for HMS (PNO: 385) from SAR Dec 2016. Retrieved from https://ebiz.acq.osd.mil/DAMIR/PurviewNew/PurviewDefault.aspx?progId=150634&subProgId=795&subType=SAR&source=urn%3aus%3amil%3aosd%3aacq%3adamir%3asar&effDate=12%2f25%2f2016&subId=167737&controlToLoad=65

Defense Acquisition University (DAU). (2013). *Defense acquisition guidebook*. Fort Belvoir, VA. Retrieved from https://acc.dau.mil/docs/dag_pdf/dag_complete.pdf

Davies, A. (2013). Graph of the week—Moore's Law. Retrieved from https://www.aspistrategist.org.au/graph-of-the-week-moores-law/

Defense Information Systems Agency (DISA). (2016). The DoDIN approved products list. Retrieved from https://aplits.disa.mil/processAPList.action

Defense Information Systems Agency (DISA). (2017). *DoDIN APL process guide v2.5*. Fort Meade, MD. Retrieved from http://www.disa.mil/~/media/Files/DISA/Services/UCCO/APL-Process/APL_Process_Guide.pdf

Defense Innovation Unit Experimental (DIUx). (2016). *DIUx commercial solutions opening how-to-guide*. Retrieved from https://www.diux.mil/CSOguide/CSOhowtoguide.pdf

Dixon, A., & Henning, J. (2013). Nett Warrior gets new end-user device. Retrieved from https://www.army.mil/article/107811

Defense Logistics Agency (DLA). (2010). *DOD acquisitions: Buying commercial items and nondevelopmental items (SD-2)*. Fort Belvoir, VA: Defense Standardization Program Office. Retrieved from http://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=112025

Department of Defense (DOD). (2009). Department of Defense Instruction 8420.01: commercial wireless local-area network (WLAN) devices, systems and technology. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/842001p.pdf

Department of Defense (DOD). (2010). *DOD unified capabilities (UC)* (No. DOD Instruction 8100.04). White House. Retrieved from http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/810004p.pdf

Department of Defense (DOD). (2011). Department of Defense (DOD) Information Technology (IT) enterprise strategy roadmap. Retrieved from http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf

Department of Defense (DOD). (2012). *DOD commercial mobile device (CMD) interim policy*. Retrieved from https://www.hsdl.org/?view&did=712435

Department of Defense (DOD). (2013). The Department of Defense Strategy for implementing the joint information environment. Retrieved from http://dodcio.defense.gov/Portals/0/Documents/JIE/2013-09-13_DOD_Strategy_for_Implmenting_JIE_(NDAA_931)_Final_Document.pdf

Department of Defense (DOD). (2015). Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS). Washington, DC: Author.

Department of Defense (DOD). (2016). Department of Defense Directive 8000.01: Management of the Department of Defense Information Enterprise (DOD IE). Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf

Department of Defense (DOD). (2017). JIDO—About. Retrieved from https://www.jieddo.mil/about.htm

Department of Defense (DOD) Chief Information Officer (CIO). (2012a). Department of Defense Mobile Device Strategy Version 2. Retrieved from http://www.dtic.mil/docs/citations/ADA560434

Department of Defense (DOD) Chief Information Officer (CIO). (2012b). Department of Defense Commercial Mobile Device (CMD) interim policy. Retrieved from https://www.hsdl.org/?view&did=712435

Department of Defense (DOD) Chief Information Officer (CIO). (2013). Department of Defense Commercial Mobile Device Implementation Plan. Retrieved from http://www.globalsecurity.org/military/library/policy/dod/dod-mobility-ip.pdf

Department of Defense (DOD) Chief Information Officer (CIO). (2014a). *Interoperability of information technology (IT) and national security systems (NSS)* (No. DOD Instruction 8330.01). Retrieved from: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/833001p.pdf

Department of Defense (DOD) Chief Information Officer (CIO). (2014b). *Cybersecurity* (No. DOD Instruction 8500.01). Washington, CD: Author. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

Department of Defense (DOD) Chief Information Officer (CIO). (2015). *Information technology standards in the DOD* (DOD Instruction 8310.01). Washington, CD: Author. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/831001p.pdf

Office of the Director, Operational Test and Evaluation (DOT&E). (2015). Nett Warrior Initial Operational and Test Evaluation (IOT&E) Report. Retrieved from http://www.dtic.mil/docs/citations/ADA626617

Eckstein, M. (2016). New Navy Procurement Office, Marines to push rapid innovation In 2016. Retrieved from https://news.usni.org/2016/03/01/new-navy-procurement-office-marines-to-push-rapid-innovation-in-2016

Egel, D., Guo, C., Lewis, J. L., & Webb, T. (2014). *Venture capital and strategic investment for developing government mission capabilities* (Prepared for the Office of the Secretary of Defense). Santa Monica, CA: RAND. Retrieved from http://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR176/RAND_RR176.pdf

Ely, C. (2014). The life expectancy of electronics. Retrieved from https://www.cta.tech/News/Blog/Articles/2014/September/The-Life-Expectancy-of-Electronics.aspx

Government Accountability Office (GAO). (2015a). *DARPA: Key factors drive transition of technologies, but better training and data dissemination can increase success* (Report to Congressional Committees No. GAO-16-5). White House. Retrieved from http://www.gao.gov/assets/680/673746.pdf

Government Accountability Office (GAO). (2015b). *Defense acquisitions: Better approach needed to account for number, cost, and performance of non-major programs* (Report to the Committee on Armed Services, House of Representatives No. GAO-15-188). White House. Retrieved from https://www.gao.gov/assets/670/668783.pdf

Government Accountability Office (GAO). (2016). *Federal acquisitions: Use of "other transaction" agreements limited and mostly for research and development activities* (Report to the Ranking Member, Committee on Science, Space, and Technology, House of Representatives). Washington, CD: Author. Retrieved from http://www.gao.gov/assets/680/674534.pdf

Giachetti, C. & Marchi, G. (2010). Evolution of firms' product strategy over the life cycle of technology-based industries: A case study of the global mobile phone industry, 1980–2009. *Business History, 52*(7), 1123–1150.

Gompert, D. C. (1999). Right makes might: Freedom and power in the Information Age. In *The changing role of information in warfare*. Santa Monica, CA: RAND. Retrieved from http://www.rand.org/pubs/monograph_reports/MR1016.html

Greene, N. (2016). Good things come in threes: BlackBerry gets key DOD certification, deployments with U.S. Coast Guard and Senate. Retrieved from http://blogs.blackberry.com/2016/07/good-things-come-in-threes-blackberry-gets-key-dod-certification-deployments-with-u-s-coast-guard-and-senate/

Government Services Agency (GSA). (2017a). Background and History. Retrieved from http://www.gsa.gov/portal/category/21354

Government Services Agency (GSA). (2017b). *Personal property disposal guide*. White House. Retrieved from https://www.gsa.gov/graphics/fas/5-06-00389_R2-yWC-w_0Z5RDZ-i34K-pR.pdf

Gutierrez, P. D. (2002). Commercial or non-developmental item acquisition strategy. *PM*, 66–68.

Halchin, E. (2011). *Other transaction (OT) authority*. Washington, DC: Congressional Research Service. Retrieved from https://fas.org/sgp/crs/misc/RL34760.pdf

Hencke, R. (2014). *Prototyping: Increasing the Pace for Innovation*. Fort Belvoir, VA: Defense Acquisition University. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA608683

Huang, A. B. (2015). The Death of Moore's Law will spur innovation. Retrieved from http://spectrum.ieee.org/semiconductors/design/the-death-of-moores-law-will-spur-innovation

iPhone Specs @ Everyiphone.com. (22 May, 2017). Retrieved from http://www.everymac.com/systems/apple/iphone/index-iphone-specs.html

Intel Corporation. (2017). 50 Years of Moore's Law. Retrieved from http://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html

Jennings, C., Wu, D., & Janis, T. (2016). Forecasting obsolescence risk and product life cycle with machine learning. *IEEE Transactions on Components, Packaging and Manufacturing Technology, 6*(9), 1428–1439.

Joint Improvised Threat Defeat Organization (JIDO). (2017). About JIDO. Retrieved from https://www.jieddo.mil/about.htm

Karalias, G. (2010). Obsolete semiconductors: A proactive approach to End-of-Life. Retrieved from http://mil-embedded.com/articles/obsolete-semiconductors-proactive-approach-end-of-life/

Kaul, V., Makaya, C., Das, S., Shur, D., & Samtani, S. (2011). On the adaptation of commercial smartphones to tactical environments. *2011 Military Communications Conference.* Retrieved from http://ieeexplore.ieee.org/document/6127649/

Koomey, J., & Naffziger, S. (2015). Moore's Law might be slowing down, but not energy efficiency. Retrieved from http://spectrum.ieee.org/computing/hardware/moores-law-might-be-slowing-down-but-not-energy-efficiency

Lin, M. J., Huang, C., & Chiang, I. (2012). Explaining trade-offs in new product development speed, cost, and quality: The case of high-tech industry in Taiwan. *Total Quality Management & Business Excellence, 23*(9/10), 1107–1123.

Lopez, T. C. (2016). CHIPS Articles: Rapid Capabilities Office to keep Army ahead of technological change. Retrieved from http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=8194

Macher, J. T., Mayo, J. W., Ukhaneva, O., & Woroch, G. (2013). Demand in a portfolio choice environment: The evolution of telecommunications. Washington, DC: Georgetown Center for Business and Public Policy, Georgetown University.

Marine Corps Warfighting Laboratory. (2009). Marine Corps Warfighting Lab (MCWL). Retrieved from https://www.afcea-qp.org/wp-content/uploads/2009/12/MCWL-Command-Brief-20091203-AFCEA.pdf

Molzahn, W. (2003). *The CIA's In-Q-Tel model: Its applicability*. Alexandria, VA: Defense Acquisition University. Retrieved from http://handle.dtic.mil/100.2/ADA423535

Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics, 38*(8), 114–116

Motorola. (2016). Maximize the Minute: PremierOne smart public safety solutions. Retrieved from https://www.motorolasolutions.com/content/dam/msi/docs/products/smart-public-safety-solutions/integrated-command-control/premierone/mot_premierone_brochure.pdf

National Information Assurance Partnership (NIAP). (2014). CCEVS Policy Letter #18. Retrieved from https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/policy-ltr-18-update2.pdf

National Information Assurance Partnership (NIAP). (2017). Production in evaluation. Retrieved from https://www.niap-ccevs.org/Product/PINE.cfm

Nidiffer, K. E., Miller, S. M., & Carney, D. (2014). *Potential use of agile methods in selected DOD acquisitions: Requirements development and management* (No.

CMU/SEI-2013-TN-006). Pittsburgh, PA: Carnegie Mellon University. Retrieved from http://repository.cmu.edu/cgi/viewcontent.cgi?article=1787&context=sei

National Institute of Standards and Technology (NIST). (2010). *Smart phone tool specification version 1.1*. Retrieved from https://www.cftt.nist.gov/documents/Smart_Phone_Tool_Specification.pdf

National Security Agency (NSA). (2016). Commercial Solutions for Classified Program (CSfC). Retrieved from https://www.nsa.gov/resources/everyone/csfc/

National Security Agency (NSA). (2017). Components list. Retrieved from https://www.nsa.gov/resources/everyone/csfc/components-list/

Oregon, R. S. (2011). *Smart fires: A COTS approach to tactical fire support using a smartphone*. Master's thesis. Retrieved from https://calhoun.nps.edu/bitstream/handle/10945/5469/11Sep_Oregon.pdf?sequence=1

Office of the Secretary of Defense (OSD). (2000). *Commercial item acquisition: Considerations and lessons learned*. White House: OSD. Retrieved from http://www.acq.osd.mil/dpap/Docs/cotsreport.pdf

Patt, D. (2013). Persistent Close Air Support (PCAS). Retrieved from http://www.darpa.mil/program/persistent-close-air-support

Perry, W. J. (1994). *Specifications & standards—A new way of doing business* (Memorandum). White House: OSD. Retrieved from http://sw-eng.falls-church.va.us/perry94.html

Phone finder and compare. (May 21, 2017). Retrieved from https://www.phonearena.com/phones/

Phone Finder. (May 23, 2017). Retrieved from http://www.gsmarena.com/search.php3?

Porche, I. R. I., McKay, S., McKernan, M., Button, R. W., Murphy, B., Giglio, K., & Axelband, E. (2012). Rapid acquisition and fielding for information assurance and cyber security in the Navy [Product Page]. Retrieved January 31, 2017, from http://www.rand.org/pubs/technical_reports/TR1294.html

Rapid Capabilities Office. (n.d.). Retrieved March 29, 2017, from http://rapidcapabilitiesoffice.army.mil/

Rapid Capabilities Office > U.S. Air Force > fact sheet display. (n.d.). Retrieved March 27, 2017, from http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104513/rapid-capabilities-office.aspx

Rai, R., & Janis, T. (2008). Principles for managing technological product obsolescence. *IEEE Transactions on Components, Packaging and Manufacturing Technology, 31*(4), 880–889.

Reinert, J. T. (2013). In-Q-Tel: The Central Intelligence Agency as venture capitalist. *Northwestern Journal of International Law & Business, 33*(3), 676–709.

Riposo, J., McKernan, M., & Duran, C. K. (2014). *Prolonged cycle times and schedule growth in defense acquisition*. Santa Monica, CA: RAND. Retrieved from http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR455/RAND_RR455.pdf

Rockwell, M. (2016). Marines could see secure handhelds by 2019. Retrieved from https://fcw.com/articles/2016/07/20/marines-secure-mobile.aspx

Small Business Administration (SBA). (2017a). Tutorial 1: What is the purpose of the SBIR & STTR programs? | SBIR.gov. Retrieved January 25, 2017, from https://www.sbir.gov/tutorials/program-basics/tutorial-1#

Small Business Administration (SBA). (2017b). Tutorial 2: Am I eligible to participate in the SBIR/STTR programs? | SBIR.gov. Retrieved January 25, 2017, from https://www.sbir.gov/tutorials/program-basics/tutorial-2#

Scarfone, K., & Souppaya, M. (2013). *NIST special publication 800–124 revision 1: Guidelines for managing the security of mobile devices in the enterprise.* Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

Scott, J., & Spaniel, D. (2016). Utilizing the NSA's CSfC process. Retrieved from http://icitech.org/wp-content/uploads/2016/07/Understanding-the-NSAs-CSFC-Process1.pdf

Seland, D. (2015). Future proofing and the death of planned obsolescence. Retrieved from http://www.qualitymag.com/articles/92652-future-proofing

Serbu, J. (2016). Navy building new office to "short-circuit" traditional DOD acquisition system. Retrieved from http://federalnewsradio.com/defense/2016/01/navy-building-new-office-short-circuit-traditional-dod-acquisition-system/

Small Business Innovation Research. (2017). About small business innovation research. Retrieved from https://www.sbir.gov/about/about-sbir

Sotire, R. B. (2010). *Web-enhanced networking: A future alternative for command and control 2025*. Master's thesis. School of Advanced Warfighting, Quantico, VA.

Souppaya, M., & Scarfone, K. (2013). *Guidelines for managing the security of mobile devices in the enterprise* (No. NIST Special Publication 800–124 Revision 1). White House: NIST. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

South, M. T. (2003). *Transitioning advanced concept technology demonstrations to acquisition programs* (Master's thesis). Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a420355.pdf

Staten, D. (2015). Marines use tablet technology to advance warfighting skills. Retrieved from http://www.marines.mil/News/News-Display/Article/624674/marines-use-tablet-technology-to-advance-war-fighting-skills/

Stevens, C. L. (2016). *An analysis of the Department of Defense's use of other transaction authority (10 U.S.C. 2371)* (Joint Applied Project). Monterey, CA: Naval Postgraduate School. Retrieved from http://calhoun.nps.edu/bitstream/handle/10945/49391/16Jun_Stevens_Catherine.pdf?sequence=1

Systems Engineering: Modular open systems approach. (2017). Retrieved from http://www.acqnotes.com/acqnote/careerfields/modular-open-systems-approach

Takai, T. M. (2012). *Cloud computing strategy*. White House: DOD. Retrieved from http://dodcio.defense.gov/Portals/0/Documents/Cloud/DOD%20Cloud%20Computing%20Strategy%20Final%20with%20Memo%20-%20July%205%202012.pdf

Tate, D. M. (2016). *Acquisition cycle time: Defining the problem*. Alexandria, VA: Institute for Defense Analysis. Retrieved from https://www.ida.org/idamedia/Corporate/Files/Publications/IDA_Documents/CARD/2016/D-5762.ashx

Thacker, M. J., & Wilson, W. W. (2015). Telephony choices and the evolution of cell phones. *Journal of Regulatory Economics*. *48*(1), 1-25

United States Congress. (1996). *Clinger Cohen Act of 1996* (No. 40 U.S.C. 1401 et seq.). White House. Retrieved from http://dodcio.defense.gov/Portals/0/Documents/ciodesrefvolone.pdf

United States Army (USA). (2007). *Army regulation 25–2: Information assurance*. Retrieved from https://ia.signal.army.mil/docs/AR25-2.pdf

United States Army (USA). (2017a). Army launches Rapid Capabilities Office. Retrieved from http://www.army.mil/article/174290/army_launches_rapid_capabilities_office

United States Army (USA). (2017b). Rapid Capabilities Office. Retrieved from http://rapidcapabilitiesoffice.army.mil/

United States Army (USA). (2017c). REF Rapid Equipping Force - United States Army. Retrieved from http://www.ref.army.mil/refhistory/

United States Air Force (USAF). (2017). Rapid Capabilities Office > U.S. Air Force > fact sheet display. Retrieved from http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104513/rapid-capabilities-office.aspx

Under Secretary of Defense (Acquisitions, Technology & Logistics). (2002). "Other Transactions" (OT) Guide for Prototype Projects. Retrieved January 26, 2017, from http://www.acq.osd.mil/dpap/Docs/policy/otherTransactions/OTA_Guide_August 2002_f00045.pdf

Under Secretary of Defense (Acquisitions, Technology & Logistics). (2007). The Defense Acquisition System (DODD 5000.01). White House: DOD.

Under Secretary of Defense (Acquisitions, Technology & Logistics). (2017). Operation of the Defense Acquisition System (DODINST 5000.02). White House: USD.

United States Marine Corps (USMC). (2010). *Integrated test and evaluation handbook*. White House. Retrieved from http://www.hqmc.marines.mil/Portals/61/Docs/MCOTEA/Signed%20USMC%20Integrated%20TE%20Handbook%20Version%201-2.pdf?ver=2012-09-28-111543-427

United States Marine Corps (USMC) (2013a). Marine Corps commercial mobile device strategy. Retrieved from http://fedne.ws/uploads/2014_APR_USMC_mobile_device_strategy.pdf

United States Marine Corps (USMC) (2013b). Marine Corps Information Enterprise Strategy Implementation Planning Guidance Version 1.1. Retrieved from http://www.hqmc.marines.mil/portals/156/newsfeeds/SV%20Documents/MCIENT_IPG_v1.1_final.pdf

United States Marine Corps (USMC) (2014). *HQMC Implementation of USMC enterprise cybersecurity directive 005 portable electronic devices*. Retrieved from http://www.hqmc.marines.mil/Portals/137/HQMC%20CYBERDIR%20005%20PED_12JUN14.PDF

United States Marine Corps (USMC) Rapid Capabilities Office (RCO). (2016). *USMC rapid capabilities office*. Presented at the NC Defense Technology Transition Symposium, North Carolina. Retrieved from http://www.ncmbc.us/docs/16DEFTECH/MarineRCO.pdf

Ward, C. D., & Sohns, C. W. (2011). Electronic component obsolescence. *IEEE Instrumentation & Measurement Magazine, 14*(6), 8–12

White House. (2012). Digital government: Building a 21st century platform to better serve the American people. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html

Wood, J. (2008). The top ten advances in materials science. *Materials Today, 11*(1-2), 40–45

Yannuzzi, R. E. (2000). In-Q-Tel: A new partnership between the CIA and the private sector. *Defense Intelligence Journal*, *9*(1), 25–37.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California